



# Pencils of quadrics and Jacobians of hyperelliptic curves

## Citation

Wang, Xiaoheng. 2013. Pencils of quadrics and Jacobians of hyperelliptic curves. Doctoral dissertation, Harvard University.

## Permanent link

<http://nrs.harvard.edu/urn-3:HUL.InstRepos:11156784>

## Terms of Use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA>

## Share Your Story

The Harvard community has made this article openly available.  
Please share how this access benefits you. [Submit a story](#).

[Accessibility](#)

Pencils of quadrics and Jacobians of hyperelliptic curves

A dissertation presented

by

Xiaoheng Wang

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University  
Cambridge, Massachusetts

March 2013

© 2012 – Xiaoheng Wang  
All rights reserved.

## Pencils of Quadrics and Jacobians of Hyperelliptic Curves

## Abstract

Using pencils of quadrics, we study a construction of torsors of Jacobians of hyperelliptic curves twice of which is  $\underline{\text{Pic}}^1$ . We then use this construction to study the arithmetic invariant theory of the actions of  $\text{SO}_{2n+1}$  and  $\text{PSO}_{2n+2}$  on self-adjoint operators and show how they facilitate in computing the average order of the 2-Selmer groups of Jacobians of hyperelliptic curves with a rational Weierstrass point, and the average order of the 2-Selmer groups of Jacobians of hyperelliptic curves with a rational non-Weierstrass point, over arbitrary number fields.

# Contents

<b>0</b>	<b>Introduction</b>	<b>1</b>
<b>1</b>	<b>Common isotropic spaces of two quadrics</b>	<b>7</b>
1.1	Odd dimension, nonsingular case . . . . .	8
1.2	Even dimension, nonsingular case . . . . .	12
1.2.1	Torsor for $J$ . . . . .	12
1.2.2	Torsor for $J[2]$ . . . . .	28
1.3	A specialization argument . . . . .	31
1.4	Odd dimension, regular case . . . . .	35
1.5	Even dimension, regular case . . . . .	45
1.5.1	Torsor for $J[2]$ . . . . .	46
1.5.2	Torsor for $J$ . . . . .	59
<b>2</b>	<b>Principal homogeneous spaces of Jacobians</b>	<b>68</b>
2.1	Weil's viewpoint . . . . .	68
2.2	Pencil of quadrics containing a rational singular quadric . . . . .	70
2.3	Orbits of an action of $\mathrm{PO}_{2n+1}$ . . . . .	71
2.4	Hyperelliptic curves with a rational Weierstrass point . . . . .	76
2.5	Quadratic refinement of the Weil pairing . . . . .	81
2.6	Pencil of quadrics containing a quadric of discriminant 1 . . . . .	84
2.7	Orbits of an action of $\mathrm{PSO}_{2n+2}$ . . . . .	86
2.8	Hyperelliptic curves with a rational non-Weierstrass point . . . . .	89
2.9	Quadratic refinement of the Weil pairing, even case . . . . .	99
2.10	Explicit computation . . . . .	101
2.10.1	Case of a rational Weierstrass point . . . . .	101
2.10.2	Case of a rational non-Weierstrass point . . . . .	108

<b>3</b>	<b>Adelic approach to orbit counting</b>	<b>110</b>
3.1	Distinguished orbits . . . . .	111
3.2	Soluble orbits . . . . .	114
3.3	Statement of the Main Theorem and integral orbits . . . . .	119
3.4	Straightening . . . . .	127
3.5	Alternative formulation for Axiom IV . . . . .	135
	<b>Reference</b>	<b>139</b>

# Acknowledgements

I am very grateful to my advisor Benedict Gross for introducing me to the subject. I would also like to thank Manjul Bhargava, George Boxer, Anand Deopurkar, Joe Harris, Wei Ho, Bao Le Hung, Anand Patel, Bjorn Poonen, Cheng-Chiang Tsai and Arul Shankar for many fruitful discussions.

## 0 Introduction

One major area of research in number theory is the study of rational points on a curve  $C$  and its Jacobian  $J$ . In 1928, Weil proved what is now known as the Mordell-Weil theorem:  $J(\mathbb{Q})$  is finitely generated as an abelian group. One important step in the proof is the finiteness of  $J(\mathbb{Q})/nJ(\mathbb{Q})$  for positive integers  $n$ . This finiteness is established by embedding  $J(\mathbb{Q})/nJ(\mathbb{Q})$  inside another finite but easier to understand group called the  $n$ -Selmer group  $\text{Sel}_n(J, \mathbb{Q})$ . The program of  $n$ -descent is precisely the study of  $J(\mathbb{Q})$  via a study of the  $n$ -Selmer group. In 1922, Mordell conjectured that the set  $C(\mathbb{Q})$  is finite when the genus of  $C$  is at least 2. Chabauty proved in 1941 that when the genus of  $C$  exceeds the rank of  $J(\mathbb{Q})$ , the set  $C(\mathbb{Q})$  is finite. Finally in 1983, Faltings settled the full Mordell conjecture using many deep tools in number theory. The general philosophy in the field is that studying  $\text{Sel}_n(J, \mathbb{Q})$  facilitates the study of  $J(\mathbb{Q})$  which in turns assists in understanding  $C(\mathbb{Q})$ .

In 2010, Manjul Bhargava and his student Arul Shankar ([5]) proved that the average rank of elliptic curves over  $\mathbb{Q}$  is bounded above by  $3/2$ , by showing that the average order of the 2-Selmer groups of elliptic curves over  $\mathbb{Q}$  is 3. This was the first time an upper bound was obtained unconditionally. Since then, they have obtained the average orders of the 3, 4, and 5-Selmer groups of elliptic curves over  $\mathbb{Q}$  thereby improving the upper bound. This thesis is concerned with generalizing the result on 2-Selmer groups to families of hyperelliptic curves over arbitrary number fields.

In Chapter 1, we develop the theory of maximal linear spaces contained in the base loci of pencils of quadrics. More precisely, let the base field  $k$  be a field of characteristic not 2. Let  $\mathcal{L} = \{xQ_1 - x'Q_2 | [x, x'] \in \mathbb{P}^1\}$  be a generic pencil of quadrics in  $\mathbb{P}^N$  and let  $B$  denote the base locus. The geometry differs significantly on the parity of  $N$ . When  $N = 2n$  is even, the dimension of maximal linear spaces contained in  $B$  is  $n - 1$ . Geometrically over  $k^s$ , there are  $2^{2n}$  such  $(n - 1)$ -planes. The arithmetic theory over  $k$  was studied in [1]. The theory when  $N = 2n + 1$  is odd is much richer. The dimension of maximal linear spaces contained in  $B$  is still  $n - 1$ . Let  $F$  denote the Fano variety of  $(n - 1)$ -planes contained in  $B$  and let  $C$  denote the



hyperelliptic curve of genus  $n$  defined by the following affine equation,

$$y^2 = (-1)^{n+1} \det(xQ_1 - Q_2).$$

It was proved by Reid [16], Desale and Ramanan [6], and Donagi [7] that geometrically over  $k^s$ ,  $F$  is isomorphic to the Jacobian  $J$  of  $C$ . As Weil pointed out in [20], Gauthier had first studied this in [8]. The main result of Chapter 1 is that over  $k$ ,  $F$  is a torsor of  $J$  and moreover,

**Theorem 1.27.** There exists a commutative algebraic group structure  $+_G$  over  $k$  on

$$G = J \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F',$$

with  $F' \simeq F$  as algebraic varieties. In particular,  $[F]$  as a class in  $H^1(k, J)$  is 4-torsion and  $2[F] = [\underline{\text{Pic}}^1(C)]$ .

In the second half of Chapter 1, we study a slight generalization of the problem where  $\mathcal{L}$  is no longer assumed to be generic, but only “regular”. The base locus will have singularities, but we still have similar results regarding the Fano variety of maximal linear spaces that miss the singularities in certain senses.

In Chapter 2, we study the conjugation actions of  $\text{PO}_{2n+1}$  and  $\text{PSO}_{2n+2}$  on self-adjoint operators on the split  $(2n+1)$ -dimensional quadric space of discriminant 1 and the split  $(2n+2)$ -dimensional quadric space, respectively. From Chapter 1 (Proposition 1.1, Proposition 1.29), we know that there is only one geometric orbit and that the stabilizer scheme of a self-adjoint operator with characteristic polynomial  $f(x)$  is canonically isomorphic to  $J[2]$ , where  $J$  is the Jacobian of the hyperelliptic curve  $C$  defined by affine equation  $y^2 = f(x)$ . Hence, the rational orbits are in bijection with

$$\ker(H^1(k, J[2]) \rightarrow H^1(k, (\text{P})\text{SO})).$$

Therefore a 2-descent analysis on  $J$  will be helpful to study these rational orbits. Depending

on the degree of  $f(x)$ ,  $C$  either has a rational Weierstrass point or a rational non-Weierstrass point. Therefore if  $\mathcal{L}$  is any pencil of quadrics whose associated hyperelliptic curve is  $C$ , the corresponding Fano variety  $F$  is a torsor of  $J$  of order 2 since  $\underline{\text{Pic}}^1(C)$  is the trivial torsor. One can then obtain a torsor of  $J[2]$  by “lifting”  $F$  to

$$F[2] = \{x \in F \mid x +_G x = (O)\},$$

where  $O$  is a point at infinity. When studying orbits of  $\text{PO}_{2n+1}$ , the hyperelliptic curve  $C$  has a rational Weierstrass point, Proposition 2.11 says that this geometric construction of torsors of  $J[2]$  exhausts all of  $H^1(k, J[2])$ . When studying orbits of  $\text{PSO}_{2n+2}$ , the hyperelliptic curve  $C$  has a rational non-Weierstrass point. In this case, we do not always exhaust  $H^1(k, J[2])$  with the pencil of quadrics construction, but we do exhaust the subset of  $H^1(k, J[2])$  that corresponds to  $\text{PSO}_{2n+2}(k)$ -orbits (Proposition 2.28).

**Theorem 2.12, 2.31.** Every element in the subgroup of  $H^1(k, J[2])$  corresponding to the image of  $J(k)/2J(k)$  under the Kummer embedding gives rise to orbits. These are called “soluble” orbits.

If one specializes to  $k$  being a number field, one can then use the Hasse principle for  $\text{PO}$  and  $\text{PSO}$  to show that

**Corollary.** There is a bijection between elements of  $\text{Sel}_2(k, J)$  and locally soluble orbits, given by the natural inclusion  $\text{Sel}_2(k, J) \hookrightarrow H^1(k, J[2])$ .

We have now completed the first step in computing the average order of 2-Selmer groups, namely the identification of 2-Selmer classes with certain orbits of coregular representations of reductive groups. The second step is to count these orbits. Bhargava and Shankar’s original approach for elliptic curves over  $\mathbb{Q}$  began by showing that every rational orbit contains an integral representative and that almost all rational orbits contain only one integral representative. Now that the problem has been reduced to counting integral orbits, they constructed a real fundamental domain and proceeded by counting the number of integral points. Due to the

non-compactness of the fundamental domain, a separate analysis of the cusps was performed. Bhargava and Gross [2] carried out this approach for hyperelliptic curves over  $\mathbb{Q}$  with a marked rational Weierstrass point, which corresponds to the action of  $\mathrm{PO}_{2n+1}$  on self-adjoint operators.

An adelic point of view was introduced by Bjorn Poonen [13]: instead of counting integral points in a real fundamental domain, one counts rational points in an adelic fundamental domain. In Chapter 3, we generalize this viewpoint to computing the average order of the  $n$ -Selmer group of families of abelian varieties satisfying four axioms. We expect that the average order has the form  $\tau_G + \gamma$  where  $\tau_G$  is the Tamagawa number of the reductive group that is acting and  $\gamma$  is, loosely speaking, the number of natural orbits. The family of Jacobians of hyperelliptic curves with a rational Weierstrass point and the family of Jacobians of hyperelliptic curves with a rational non-Weierstrass point both satisfy the four axioms. We expect that:

**Conjecture 5.** The average order of the 2-Selmer group of the Jacobians of hyperelliptic curves of genus  $n$  over a number field  $k$  with a rational Weierstrass point is 3. In particular, the average rank of the Jacobians of such hyperelliptic curves is bounded by  $3/2$ .

**Conjecture 6.** The average order of the 2-Selmer group of the Jacobians of hyperelliptic curves of genus  $n$  over a number field  $k$  with a rational non-Weierstrass point is 6. In particular, the average rank of such hyperelliptic curves is bounded by  $5/2$ .

## Notations and conventions

We list some of the notations and conventions we follow. Most of them will be stated again in the passing.

### Linear structure

Throughout,  $k$  will be a perfect field of characteristic not 2. Let  $k^s = k^a$  be an algebraic closure of  $k$ .

Let  $U$  denote some ambient vector space over  $k$ . Denote its projective variety of lines by  $\mathbb{P}U$

viewed as an algebraic variety over  $k$ . For any field  $k'$  containing  $k$ , we write  $X \subset_{k'} U$  if  $X$  is a linear  $k'$ -subspace of  $U \otimes k'$  and write  $X \subset U$  when  $k' = k^s$ . The projectivization of  $X$  is denoted by  $\mathbb{P}X \subset \mathbb{P}U$ , and we write

$$\dim(X) = n, \quad \dim(\mathbb{P}X) = n - 1.$$

If  $v \in U \otimes k^s$ , denote by  $[v]$  the point in  $\mathbb{P}U$  corresponding to the line spanned by  $v$ .

For any  $n$ , one has the following two algebraic varieties over  $k$ ,

$$\begin{aligned} Gr(n, U) &= \{X \subset U \mid \dim(X) = n\}, \\ \mathbb{G}r(n, \mathbb{P}U) &= \{\mathbb{P}X \subset \mathbb{P}U \mid \dim(\mathbb{P}X) = n\}. \end{aligned}$$

If  $B \subset \mathbb{P}U$  is an algebraic variety and  $p \in B$ , denote by  $T_p B \subset \mathbb{P}U$  the projective tangent space. If  $X$  is a subset of  $B(k^s)$ , we define  $T_X B$  as

$$T_X B = \bigcap_{p \in X} T_p B.$$

## Quadratic structure

We will use  $Q$  to denote a quadratic form on  $U$ , a quadratic form on  $U \otimes k^s$  via extension of scalars, and a quadric in  $\mathbb{P}U$ . Its associated bilinear form, denoted  $b$ , is defined by

$$b(v, w) = \frac{1}{2}(Q(v + w) - Q(v) - Q(w)), \forall v, w \in U \otimes k^s.$$

The quadratic form  $Q$  can be recovered from  $b$  via  $Q(v) = b(v, v)$ . Its discriminant differs from its determinant by  $(-1)^n$  if  $\dim(U) = 2n + 1$  and by  $(-1)^{n+1}$  if  $\dim(U) = 2n + 2$ .

For any  $X \subset_{k'} U$ , denote the following subspace by  $X^{\perp_Q}$  or by  $X^\perp$  if  $Q$  is clear from the context,

$$X^{\perp_Q} = \{v \in U \otimes k' \mid b(x, v) = 0, \forall x \in X\}.$$

A linear subspace  $X \subset_{k'} U$  is **isotropic** with respect to  $Q$  if  $X \subset X^{\perp_Q}$ , or equivalently  $\mathbb{P}X \subset Q \subset \mathbb{P}U$ . In this case,

$$T_{\mathbb{P}X}Q = \mathbb{P}(X^{\perp_Q}).$$

If  $T$  is a linear operator on  $U \otimes k^s$ , we denote its adjoint operator by  $T^*$ . That is,

$$b(Tv, w) = b(v, T^*w).$$

## Galois structure

A linear subspace  $X$  of  $U \otimes k^s$  is defined over  $k$  if it admits a  $k^s$ -basis consisting of vectors in  $U$ . A linear subspace  $\mathbb{P}X \subset \mathbb{P}U$  is defined over  $k$  if  $X$  is defined over  $k$ . A linear operator  $T$  on  $U \otimes k^s$  is defined over  $k$  if it preserves  $U$ . A quadratic form  $Q$  on  $U \otimes k^s$ , is defined over  $k$  if  $Q(U) \subset k$ .

As we will be mostly working with quadratic forms over fields of characteristic not 2, almost every object will be defined over  $k^s$ . For any algebraic group  $G$  over  $k$ , we write  $H^i(k, G)$  for  $H^i(\text{Gal}(k^s/k), G(k^s))$ . Two 1-cocycles  $(b_\sigma)_\sigma, (c_\sigma)_\sigma$  are cohomologous if there exists some  $g \in G(k^s)$  such that

$$b_\sigma = g^{-1}c_\sigma^\sigma g, \forall \sigma \in \text{Gal}(k^s/k).$$

## Acknowledgements

I am very grateful to my advisor Benedict Gross for introducing me to the subject. I would also like to thank Manjul Bhargava, George Boxer, Anand Deopurkar, Joe Harris, Wei Ho, Bao Le Hung, Anand Patel, Bjorn Poonen, Cheng-Chiang Tsai and Arul Shankar for many fruitful discussions.

# 1 Common isotropic spaces of two quadrics

Let  $k$  be a perfect field of characteristic not 2 and let  $Q_1, Q_2$  be two linearly independent quadratic forms on a  $k$ -vector space  $U$ . In this chapter, we study the general geometry of the maximal isotropic subspaces with respect to both quadrics.

There are three equivalent ways to formulate this problem. We call the above formulation the  $(Q_1, Q_2)$ -setup. Suppose now  $Q_1$  is non-degenerate. Let  $b_1, b_2$  denote the corresponding bilinear form,

$$b_i(v, w) = \frac{1}{2}(Q_i(v + w) - Q_i(v) - Q_i(w)).$$

Let  $T : U \rightarrow U$  be the unique operator such that for all  $v, w \in U$ ,

$$b_2(v, w) = b_1(v, Tw). \tag{1.1}$$

Note  $T$  is self-adjoint with respect to  $b_1$  since  $b_1, b_2$  are symmetric.

To say a linear subspace  $X$  is isotropic with respect to both  $Q_1, Q_2$  is the same as saying

$$X \subset X^{\perp_{Q_1}}, TX \subset X^{\perp_{Q_1}}. \tag{1.2}$$

Therefore, instead of starting with a pair of quadratic forms, we could have started with a non-degenerate quadratic form along with a self-adjoint operator. We call this formulation the  $(Q_1, T)$ -setup.

Lastly, we could view  $Q_1, Q_2$  as quadrics in  $\mathbb{P}U$  and take a pencil  $\mathcal{L} = \{xQ_1 - yQ_2 \mid [x, y] \in \mathbb{P}^1\}$  of quadrics in  $\mathbb{P}U$ . Let  $B = Q_1 \cap Q_2$  denote the base locus. The above problem regarding common isotropic subspaces translates into studying the variety of maximal dimensional linear subspaces contained in the base locus. We call this formulation the  $(\mathbb{P}U, \mathcal{L})$ -setup.

The geometry depends very much on the parity of the dimension of  $U$  and we shall study them separately in what follows. As we will discover, Jacobians of certain hyperelliptic curves play important roles.

When there is an algebraic group  $G$  acting on an algebraic variety  $Y$  over  $k$ , we say  $Y$  is a torsor for  $G$  if for every field  $k'$  containing  $k$ , the action of  $G(k')$  on  $Y(k')$  is simply-transitive. In Section 1.3, we show that the torsors constructed in what follows are torsors in the conventional sense. That is, the morphism  $G \times X \rightarrow X \times X$  induced from the action of  $G$  on  $X$  is an isomorphism.

## 1.1 Odd dimension, nonsingular case

Suppose  $U$  has dimension  $2n + 1$ . We first define what we mean by “nonsingular” in each of the three formulations. With the  $(Q_1, Q_2)$ –setup, we require  $f_0(x) = (-1)^n \det(xQ_1 - Q_2)$  to have no repeated roots. With the  $(Q, T)$ –setup, we require the characteristic polynomial  $f_T(x) = \det(xI - T)$  of the self-adjoint operator  $T$  to have no repeated roots. With the  $(\mathbb{P}U, \mathcal{L})$ –setup, we require that the pencil  $\mathcal{L}$  is generic in the sense of Donagi [7]. Namely, apart from  $2n + 1$  simple cones in  $\mathcal{L}$ , a general member of  $\mathcal{L}$  is a smooth quadric. This is also equivalent to requiring that

$$y^2 = f_0(x) = (-1)^n \det(xQ_1 - Q_2)$$

defines a hyperelliptic curve of genus  $n$ . We also assume that the polynomials  $f_0, f_T$  split completely over  $k^s$ .

The classical geometry over  $k^s$  is fairly well-known using intersection theory. We give a brief sketch of the argument and refer to [7, §1.2] for the complete treatment.

For a smooth quadric  $Q$  in  $\mathbb{P}^{2n}$ , the maximal dimensional linear subspace contained in it has dimension  $n - 1$ . The Lagrangian variety  $L_Q$  of  $Q$  defined by

$$L_Q = \{\mathbb{P}X \mid \mathbb{P}X \subset Q, \dim(\mathbb{P}X) = n - 1\} \subset \mathbb{G}r(n - 1, 2n)$$

has dimension  $n(n + 1)/2$ , which is precisely half the dimension of  $\mathbb{G}r(n - 1, 2n)$ . If  $Q_1, Q_2$  span a generic pencil, then  $L_{Q_1}$  and  $L_{Q_2}$  intersect transversely in  $\mathbb{G}r(n - 1, 2n)$ . In the Chow ring of  $\mathbb{G}r(n - 1, 2n)$ , the class of  $L_{Q_i}$  is  $2^n \sigma_{n, n-1, \dots, 1}$  in the notation of Schubert calculus. The class

$\sigma_{n,n-1,\dots,1}$  has self intersection 1. Therefore  $L_{Q_1} \cap L_{Q_2}$  is a discrete set of  $2^{2n}$  points. In other words, there are precisely  $2^{2n}$   $(n-1)$ -planes defined over  $k^s$  contained in the base locus  $Q_1 \cap Q_2$ .

The arithmetic aspect of the theory has been studied by Bhargava and Gross in [1], we include much of the discussion here in this section for completeness and to set some notations for later sections. We will adopt the  $(Q, T)$ -setup for this case. Just to recall notation,  $Q$  is a non-degenerate quadratic form on  $U$  defined over  $k$  and  $T$  is a self-adjoint operator with respect to  $Q$ . The characteristic polynomial  $f_T(x)$  of  $T$  has no repeated factors. For every field  $k'$  containing  $k$ , let  $W_T(k')$  denote the set of (linear)  $n$ -dimensional  $k'$ -subspaces  $X$  of  $U \otimes k'$  such that  $X \subset X^\perp, TX \subset X^\perp$ .

As it turns out, it is more convenient to let  $T$  vary as well. Let  $f(x)$  be a separable monic polynomial of degree  $2n+1$  over  $k$ . Consider the following two schemes over  $k$ .

$$V_f = \{T : U \rightarrow U \mid T^* = T \text{ with characteristic polynomial } f\} \subset \mathbb{A}^{(2n+1)^2},$$

$$W_f = \{(T, X) \in V_f \times Gr(n, U) \mid X \subset X^\perp, TX \subset X^\perp\}.$$

The group  $\text{PO}(U, Q) = O(U, Q)/(\pm 1)$  acts on  $V_f, W_f$  via

$$g.T = gTg^{-1}, \quad g.(T, X) = (gTg^{-1}, gX).$$

**Proposition 1.1.** If  $f(x)$  splits completely over  $k$  and  $k = k^2$ , for example  $k = k^s$ , then  $\text{PO}(U, Q)(k)$  acts transitively on  $V_f(k)$ . For general  $k$ , suppose  $T \in V_f(k')$  is defined over some field  $k'$  containing  $k$ . Then its stabilizer scheme  $\text{Stab}(T)$  is isomorphic to  $\text{Res}_{L'/k'} \mu_2 / \mu_2$  as group schemes over  $k'$  where  $L' = k'[x]/f(x)$ .

**Proof:** For any  $T$  in  $V_f(k')$ , since  $T$  is regular semi-simple, its stabilizer scheme in  $\text{GL}(U_{k'})$  is a maximal torus. It contains and hence equals to the maximal torus  $\text{Res}_{L'/k'} \mathbb{G}_m$ . For any



$k'$ -algebra  $K$ ,

$$\begin{aligned}\text{Stab}_{O(U_{k'}, Q)}(T)(K) &= \{g \in (K[T]/f(T))^\times \mid g^*g = 1\} \\ &= \{g \in (K[T]/f(T))^\times \mid g^2 = 1\}.\end{aligned}$$

Hence  $\text{Stab}_{O(U_{k'}, Q)}(T) \simeq \text{Res}_{L'/k'} \mu_2$  and  $\text{Stab}_{PO(U_{k'}, Q)}(T) \simeq \text{Res}_{L'/k'} \mu_2 / \mu_2$ .

Suppose now  $f(x)$  splits completely in  $k$  and  $k = k^2$ . Suppose  $T_1, T \in V_f(k)$ . We claim they can be conjugated to each other by an element of  $\text{PO}(U, Q)(k)$ . There exists  $g \in GL(U)(k)$  such that  $T_1 = gTg^{-1}$ . Since  $T_1$  and  $T$  are both self-adjoint,  $g^*g$  centralizes  $T$  and hence lies in  $(k[T]/f(T))^\times$ . Since  $f$  splits over  $k$ ,  $(k[T]/f(T))^\times$  is a product of  $k^\times$ . Since  $k = k^2$ , there exists  $h \in (k[T]/f(T))^\times$  such that  $g^*g = h^2$ . Now  $gh^{-1}$  is an element of  $O(U, Q)(k)$  conjugating  $T$  to  $T_1$ . Its image in  $\text{PO}(U, Q)(k)$  does the job.  $\square$

For general  $Q$ , there might not be a self-adjoint operator defined over  $k$  with the prescribed characteristic polynomial. For example over  $\mathbb{R}$ , operators self-adjoint with respect to the positive definite form have real eigenvalues.

**Lemma 1.2.** If  $Q$  is split, then  $V_f(k)$  and  $W_f(k)$  are nonempty. Furthermore, there exists  $(T_0, X_0) \in W_f(k)$  with trivial stabilizer in  $\text{PO}(U, Q)(k^s)$ .

**Proof:** Consider the  $2n + 1$  dimensional étale  $k$ -algebra  $L = k[x]/f(x)$ . When viewed as a vector space over  $k$ ,  $L$  has a power basis  $\{1, \beta, \dots, \beta^{2n}\}$  where  $\beta \in L$  is the image of  $x$ . On  $L$  there is the following bilinear form

$$\langle \lambda, \mu \rangle = \text{coefficient of } \beta^{2n} \text{ in } \lambda\mu / \text{disc}(Q) = \text{Tr}(\lambda\mu / (\text{disc}(Q) \cdot f'(\beta))),$$

where the second equality is due to Euler ([?, §III.6 Lemma 2]). This form defines a split quadratic form since  $X = \text{Span}_k\{1, \beta, \dots, \beta^{n-1}\}$  is a rational maximal isotropic subspace. When expressed in the basis  $\{1, \beta, \dots, \beta^{2n}\}$ , the Gram matrix of this form has non-zero entries only on and to the right of the anti-diagonal and every element on the anti-diagonal is equal to  $1/\text{disc}(Q)$ .

Therefore, its discriminant is also  $\text{disc}(Q)$  modulo squares. Hence there exists an isometry from  $(L, \langle, \rangle)$  to  $(U, Q)$  defined over  $k$ . Via this identification, the operator  $\cdot\beta$  on  $L$  transforms into a self-adjoint operator  $T_0$  on  $U$ . Denote by  $X_0$  the image of  $X$  under this isometry. The stabilizer of  $(\cdot\beta, X)$  in  $\text{GL}(L)(k^s)$  consists of polynomials in  $\beta$  that stabilizes  $X$ . Hence the corresponding element  $(T_0, X_0) \in W_f(k)$  has trivial stabilizer in  $\text{PO}(U, Q)(k^s)$ .  $\square$

**Theorem 1.3.** Suppose  $k$  is separably closed. Then  $\text{PO}(V, Q)(k)$  acts simply-transitively on  $W_f(k)$ .

**Proof:** Since  $Q$  is split over  $k$ , Proposition 1.1 implies that it suffices to prove that for the  $T_0 \in V_f(k)$  obtained in the above lemma,  $\text{Stab}(T_0)(k)$  acts simply-transitively on  $W_{T_0}(k)$ . Since  $(T_0, X_0)$  has trivial stabilizer, it suffices to show that  $\text{Stab}(T_0)(k)$  and  $W_{T_0}(k)$  have the same size. As we saw above,  $W_T(k^s)$  has  $2^{2n}$  elements for any  $T$ . Hence we are done because  $2^{2n} = |\text{Res}_{L/k}\mu_2/\mu_2(k)|$ .  $\square$

**Theorem 1.4.** Suppose  $k$  is arbitrary and  $W_f(k)$  is non-empty. Then  $\text{PO}(V, Q)(k')$  acts simply-transitively on  $W_f(k')$  for any field  $k'$  containing  $k$ .

**Proof:** It suffices to prove transitivity. Suppose  $(T_1, X_1), (T_2, X_2) \in W_f(k')$ , let  $g \in \text{PO}(V, Q)(k'^s)$  be the unique element sending  $(T_1, X_1)$  to  $(T_2, X_2)$ . Then for any  $\sigma \in \text{Gal}(k'^s/k')$ ,  ${}^\sigma g$  also sends  $(T_1, X_1)$  to  $(T_2, X_2)$ . Hence  $g = {}^\sigma g \in \text{PO}(V, Q)(k')$ .  $\square$

**Corollary 1.5.** Suppose  $k$  is arbitrary, and  $T \in V_f(k)$ . Let  $J$  denote the Jacobian of the hyperelliptic curve defined by  $y^2 = f(x)$ . Then there is an action of  $J[2]$  on  $W_T$  such that for any field  $k'$  containing  $k$ ,  $J[2](k')$  acts simply-transitively on  $W_T(k')$ .

**Proof:** It is immediate from Theorem 1.4 that  $\text{Stab}(T)(k')$  acts simply-transitively on  $W_T(k')$  for any field  $k'$  containing  $k$ . Proposition 1.1 says, as group schemes over  $k$ ,

$$\text{Stab}(T) \simeq \text{Res}_{L/k}\mu_2/\mu_2 \simeq (\text{Res}_{L/k}\mu_2)_{N=1} \simeq J[2], \quad (1.3)$$

where  $L = k[x]/f(x)$ .  $\square$

**Remark 1.6.** One can write down an explicit formula for the above identification of  $J[2]$  with  $\text{Stab}(T)$ . We will work over  $k^s$  and it will be clear that the map is Galois equivariant. Denote the roots of  $f(x)$  over  $k^s$  by  $\alpha_1, \dots, \alpha_{2n+1}$ , and by  $P_i$  the Weierstrass point corresponding to the root  $\alpha_i$ . Recall  $J[2]$  is an elementary 2-group generated by  $(P_i) - (\infty)$  with the only relation being that their sum is trivial, cf. (2.7). For each generator  $(P_i) - (\infty)$ , one looks for a polynomial  $g_i(x)$  such that  $g_i(\alpha_i) = -1$  and  $g_i(\alpha_j) = 1$  for all  $j \neq i$ . Then  $g_i(T)$  is the image of  $(P_i) - (\infty)$  in  $\text{Stab}(T)$ . The image does not depend on the choice of the polynomial  $g_i$  because any two choices differ by some multiples of  $f(x)$  and  $f(T) = 0$ . Define  $h_i(x) = f(x)/(x - \alpha_i)$ , then

$$g_i(x) = 1 - 2 \frac{h_i(x)}{h_i(\alpha_i)}$$

does the job. In other words, on the level of  $k^s$ -points, (1.3) is given by

$$\sum ((\alpha_i) - (\infty)) \mapsto \prod \left( 1 - 2 \frac{h_i(T)}{h_i(\alpha_i)} \right) = 1 - 2 \sum \frac{h_i(T)}{h_i(\alpha_i)}.$$

The above summation and product are written without indices, meaning the above equality holds for any (finite) collection of matching indices.

See Remark 2.8 for a different view point of (1.3).

## 1.2 Even dimension, nonsingular case

### 1.2.1 Torsor for $J$

Suppose  $U$  has dimension  $2n + 2$ . The projective formulation is easier to work with in this case.

Let  $\mathcal{L} = \{Q_\lambda | \lambda \in \mathbb{P}^1\}$  be a rational generic pencil of quadrics in  $\mathbb{P}^{2n+1} = \mathbb{P}U$ . Rationality means it is generated by two quadrics  $Q_1, Q_2$  defined over  $k$ . The following equivalent conditions give the definition for genericness. See [7, §1.2] for the proof.

**Lemma 1.7.** The following conditions are equivalent.

1. The generic members of  $\mathcal{L}$  are smooth quadrics. There are precisely  $2n+2$  singular quadrics

in  $\mathcal{L}(k^s)$ , they are all simple cones.

2. The following affine equation

$$C : y^2 = (-1)^{n+1} \det(xQ_1 - Q_2)$$

defines a hyperelliptic curve of genus  $n$ .

3. The base locus  $B = Q_1 \cap Q_2$  is a smooth.

The cone points of the  $2n+2$  singular quadrics are best understood in terms of the self-adjoint operator  $T$  defined in (1.1) assuming  $Q_1$  is non-degenerate. The quadric  $\lambda Q_1 - Q_2$  is singular if and only if  $\lambda$  is an eigenvalue of  $T$ . If we denote a corresponding eigenvector by  $v_\lambda$ , then the cone point of  $\lambda Q_1 - Q_2$  is  $[v_\lambda] \in \mathbb{P}U$ . In particular, the  $2n+2$  cone points span the entire  $\mathbb{P}U$ .

Since  $\mathcal{L}$  is generic, the maximal (projective) dimension of any linear space contained in the base locus  $B$  is  $n-1$  ([7, Corollary 1.5]). Consider the following variety over  $k$ ,

$$F = \{\mathbb{P}X | \dim(\mathbb{P}X) = n-1, \mathbb{P}X \subset B\}.$$

### The hyperelliptic curve $C$

For any rational generic pencil  $\mathcal{L}$ , there is an *associated hyperelliptic curve* defined as follows.

For any quadric  $Q$  in  $\mathbb{P}^{2n+1}$ , one defines its Lagrangian variety by

$$L_Q = \{\mathbb{P}Y | \mathbb{P}Y \subset Q, \dim(\mathbb{P}Y) = n\} \subset \mathbb{G}r(n, \mathbb{P}U).$$

When  $Q$  is smooth,  $L_Q$  has two connected components, also called the **rulings** of  $n$ -planes in  $Q$ . Two  $n$ -planes in  $Q$  lie in the same ruling if and only if their intersection codimension in either one of them is even. If  $Q$  is defined over some field  $k'$ , its **discriminant** is defined by

$$\text{disc}(Q) = (-1)^{n+1} \det(Q) k'^{\times 2} \in k'^{\times} / k'^{\times 2}.$$

The connected components of  $L_Q$  are defined over  $k'(\sqrt{\text{disc}(Q)})$ . In other words,  $L_Q(k'^s)$  hits both rulings and the  $\text{Gal}(k'^s/k'(\sqrt{\text{disc}(Q)}))$ -action on  $L_Q(k'^s)$  preserves the rulings. When  $Q$  is singular,  $L_Q$  has only one connected component.

Consider the following variety

$$\tilde{F} = \{(Q_\lambda, \mathbb{P}Y) | \lambda \in \mathbb{P}^1, \mathbb{P}Y \in L_{Q_\lambda}\} \subset \mathcal{L} \times \mathbb{G}r(n, \mathbb{P}U).$$

There is an obvious projection map  $p_1 : \tilde{F} \rightarrow \mathbb{P}^1$ . The fiber over  $\lambda \in \mathbb{P}^1$  is isomorphic to  $L_{Q_\lambda}$ . Let

$$\epsilon : \tilde{F} \rightarrow C, \quad \pi : C \rightarrow \mathbb{P}^1$$

denote the Stein factorization. In other words,  $\epsilon$  has connected fibers and the fibers of  $\pi$  correspond bijectively to the connected components of the fibers of  $p_1$ . Therefore,  $C$  is a double cover of  $\mathbb{P}^1$  branched over the  $2n + 2$  points that correspond to the singular quadrics on the pencil. A homogeneity analysis as in [7, Lemma 1.6] shows that  $C$  is smooth at the ramification points. Hence  $C$  is a hyperelliptic curve of genus  $n$ , and to give a point on  $C$  is the same as giving a quadric on the pencil plus a choice of ruling. We call  $C$  the hyperelliptic curve associated to the pencil and it parameterizes the rulings in the pencil. The Weierstrass points of  $C$  correspond to the  $2n + 2$  points on  $\mathbb{P}^1$  cut out by  $\det(xA_1 - yA_2)$ . The curve  $C$  is isomorphic over  $k$ , but not canonically, to the hyperelliptic curve defined by the affine equation

$$y^2 = (-1)^{n+1} \det(xA_1 - A_2).$$

It was known to algebraic geometers ([16], [6], [7]) that when  $k$  is algebraically closed,  $F$  is isomorphic to  $J$ , the Jacobian of the curve  $C$  defined above. Therefore it is natural to expect that over a general field,  $F$  is a torsor of  $J$ . In fact, we prove something stronger:

**Theorem 1.8.** Let  $G$  be the disconnected variety

$$G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F',$$

where  $F'$  is a copy of  $F$ . There is a commutative algebraic group structure  $+_G$  on  $G$  over  $k$  such that,

1.  $G^0 = \underline{\text{Pic}}^0(C)$  with component group  $G/G^0 \simeq \mathbb{Z}/4\mathbb{Z}$ ,
2.  $F'$  is isomorphic to  $F$  as varieties via the inversion map  $-1_G$ ,
3. the group law extends that on  $H = \underline{\text{Pic}}(C)/\mathbb{Z}D_0 \simeq \underline{\text{Pic}}^0(C) \dot{\cup} \underline{\text{Pic}}^1(C)$  where  $D_0$  is the hyperelliptic class.

Moreover, we will show that this structure is unique once we impose one more condition. See Theorem 1.27 for the complete statement.

### The dimension of $F$

From the result over the algebraic closure, one can conclude that  $F$  has dimension  $n$  as an algebraic variety. Even without passing to the algebraic closure, one can still show that  $F$  has dimension at least  $n$ . For any quadric  $Q$  in  $\mathbb{P}^{2n+1}$ , let  $F_{n-1,Q}$  denote the variety of  $(n-1)$ -planes in  $Q$ . When  $Q$  is smooth,  $F_{n-1,Q}$  is smooth irreducible of dimension  $n(n+3)/2$  ([9] p.293). Let  $Q, Q'$  be two smooth quadrics on the pencil, then  $F = F_{n-1,Q} \cap F_{n-1,Q'}$  has dimension at least

$$n(n+3)/2 + n(n+3)/3 - \dim \text{Gr}(n-1, 2n+1) = n.$$

### The morphism $\tau : C \times F \rightarrow F$ .

Given any pair  $(c, \mathbb{P}X) \in C \times F$ , there is a unique  $n$ -plane  $\mathbb{P}Y$  containing  $\mathbb{P}X$  in the ruling of the quadric defined by  $c$ . Let  $Q$  be another quadric in the pencil. Since the base locus contains no  $n$ -planes,  $\mathbb{P}Y \cap B = \mathbb{P}Y \cap Q$  is a quadric in  $\mathbb{P}Y$  containing  $\mathbb{P}X$ . Hence,  $\mathbb{P}Y \cap B = \mathbb{P}X \cup \mathbb{P}X'$  is the union of two possibly equal  $(n-1)$ -planes. We define  $\tau(c, \mathbb{P}X)$  to be  $\mathbb{P}X'$ . (See Lemma 1.35 for the proof that  $\tau$  is a morphism.)

For a fixed  $c \in C$ , define  $\tau(c) : F \rightarrow F$  by  $\tau(c)\mathbb{P}X = \tau(c, \mathbb{P}X)$ . Note  $\tau(c)$  is an involution in the sense  $\tau(c)^2 = \text{id}$ .

We can write down a more explicit formula for  $\tau$  as follows. Given any  $(c, \mathbb{P}X) \in C \times F$ , let  $\mathbb{P}Y$  denote the unique  $n$ -plane containing  $\mathbb{P}X$  in the ruling of the quadric specified by  $c$ . Since  $\mathbb{P}Y \not\subseteq Q$ , there exists  $p \in Y \setminus X$  such that  $b(p, p) \neq 0$  where  $b$  is the bilinear form associated to  $Q$ . There is a linear map on  $U \times k^s$  given by reflection about  $p^{\perp_Q}$ , namely

$$\text{refl}_p : v \mapsto v - 2 \frac{b(v, p)}{b(p, p)} p.$$

Then

$$\tau(c, \mathbb{P}X) = \mathbb{P}(\text{refl}_p(X)).$$

In order to put a group structure on  $G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F'$ , it suffices to define a simply-transitive action of  $H = \underline{\text{Pic}}(C)/\mathbb{Z}D_0$  on  $F \dot{\cup} F'$  for then one can define  $+_G$  as follows: for any  $x, x' \in F \dot{\cup} F'$ ,  $[D], [D'] \in H$ :

1.  $[D] +_G [D']$  is the usual addition in  $H$ ,
2.  $x +_G [D] = x + [D]$  is the image of  $x$  under the action of  $[D]$ ,
3.  $x +_G x'$  is the unique element in  $H$  that sends  $-x'$  to  $x$ .

### **An action of $\text{Div}(C)$ on $F \dot{\cup} F'$**

We start from the following action of  $C$  on  $F \dot{\cup} F'$ :

$$\mathbb{P}X + (c) = -\tau(\bar{c})\mathbb{P}X, \quad -\mathbb{P}X + (c) = \tau(c)\mathbb{P}X, \quad (1.4)$$

where  $c \mapsto \bar{c}$  denotes the hyperelliptic involution. The second equality follows the idea that  $\tau : C \times F \rightarrow F$  serves as a subtraction, and the first equality was rigged so that divisors linearly equivalent to the hyperelliptic class  $D_0$  acts trivially. The following Lemma allows one to extend this action to the semi-group of effective divisors on  $C$ . Negating (1.4) then gives the extension to the entire group of divisors.

**Lemma 1.9.** For any  $x \in F \dot{\cup} F'$ ,  $c_1, c_2 \in C$ ,

$$(x + (c_1)) + (c_2) = (x + (c_2)) + (c_1).$$

**Proof:** Unwinding the above definition, we need to prove for any  $\mathbb{P}X \in F$ ,

$$\tau(c_2)\tau(\overline{c_1})\mathbb{P}X = \tau(c_1)\tau(\overline{c_2})\mathbb{P}X.$$

As both sides are defined by polynomial equations, it suffices to prove this equality for generic  $\mathbb{P}X, c_1, c_2$ , over the algebraic closure, in particular we may assume there is no tangency involved. This is proved in [7, p.232] by looking at the following intersection

$$\text{Span}\{\mathbb{P}X, \tau(\overline{c_1})\mathbb{P}X, \tau(\overline{c_2})\mathbb{P}X\} \cap B. \quad \square$$

**Theorem 1.10.** The above action of  $\text{Div}(C)$  descends to a simply-transitive action of  $H$  on  $F \dot{\cup} F'$ .

**Remark 1.11.** 1.  $+_G$  is defined over  $k$ , because  $\tau$  is defined over  $k$ .

2.  $+_G$  is commutative. If  $[D]$  sends  $-x'$  to  $x$ , it also sends  $-x$  to  $x'$ . This follows from the definition of the action of  $\text{Div}(C)$  on  $F \dot{\cup} F'$ .
3. The action  $\tau$  and the group law  $+_G$  are defined on the level of points. This is the main reason why we are using a weaker version of the notion of “torsor”. We will show that  $+_G$  is a morphism  $G \times G \rightarrow G$ . More work needs to be done to rule out inseparable isogeny in characteristic  $p$ . We deal with these technical issues in Section 1.3.

Before proving this Theorem, we give some concrete examples of  $+_G$  in certain simple cases.

**Example 1.12.** Suppose  $n = 1$ . Then  $F$  is the variety of points in the intersection of two generic quadrics in  $\mathbb{P}^3$  and  $C$  is a genus 1 curve. Given two points  $\mathbb{P}X, \mathbb{P}X' \in F$ , let  $\mathbb{P}Y$  denote the line passing through them. There exists a unique quadric in the pencil and a unique ruling that



contains  $\mathbb{P}Y$ , and this data is equivalent to giving a point on  $C$ . If one passes to the algebraic closure and identify  $F \simeq J \simeq C$ , then  $+_G : F \times F \rightarrow \underline{\text{Pic}}^1(C)$  is just the addition on  $J$ .

**Example 1.13.** Suppose now  $n$  is general and  $\mathbb{P}X, \mathbb{P}X' \in F$  intersect in codimension 1 in either/both of them. Let  $\mathbb{P}Y = \text{Span}\{\mathbb{P}X, \mathbb{P}X'\}$  denote their linear span, then  $\mathbb{P}Y \simeq \mathbb{P}^n$ . Let  $p$  be a point on  $\mathbb{P}Y \setminus (\mathbb{P}X \cup \mathbb{P}X')$ . There is a quadric  $Q$  in  $\mathcal{L}$  containing  $p$ . Its intersection with  $\mathbb{P}Y$  contains two  $\mathbb{P}^{n-1}$  and a point not on them, hence it cannot be a quadric. Furthermore, since the pencil is generic, the base locus contains no  $\mathbb{P}^n$ . Therefore,  $\mathbb{P}Y$  is contained in a unique quadric  $Q$  in  $\mathcal{L}$  and a unique ruling on  $Q$ . Once again, such data determines a point on  $c \in C$  and our group law says

$$\mathbb{P}X +_G \mathbb{P}X' = (c) \in \underline{\text{Pic}}^1(C).$$

**Example 1.14.** For any  $\mathbb{P}X \in F$ , since  $B$  is a complete intersection,

$$T_{\mathbb{P}X}B = T_{\mathbb{P}X}Q_1 \cap T_{\mathbb{P}X}Q_2 = \mathbb{P}(X^{\perp_{Q_1}} \cap X^{\perp_{Q_2}}).$$

As the next Lemma shows,  $T_{\mathbb{P}X}B$  has dimension at most  $n$ . If  $\mathbb{P}X \in F$  such that  $T_{\mathbb{P}X}B \simeq \mathbb{P}^n$ , then just as in the above example, there exist a unique quadric in  $\mathcal{L}$  and a unique ruling that contains  $T_{\mathbb{P}X}B$ . Such data determines a point on  $c \in C$  and our group law says

$$\mathbb{P}X +_G \mathbb{P}X = (c) \in \underline{\text{Pic}}^1(C).$$

However, it is not a priori clear that there even exists  $\mathbb{P}X$  for which  $T_{\mathbb{P}X}B$  is not just  $\mathbb{P}X$ . Luckily, each singular quadric gives rise to  $2^{2n}$  of them (defined over  $k^a$ ). Indeed, let  $P_i$  be a Weierstrass point on  $C$  corresponding to a singular quadric  $Q_{\lambda_i}$ , let  $p_i$  denote the vertex of this simple quadric cone. Notice the hyperplane

$$H = \mathbb{P}(p_i^{\perp_{Q_{\lambda_i}}})$$

does not depend on the choice of the quadric  $Q_{\lambda}$  as  $T_{p_i}Q_{\lambda_i} = \mathbb{P}^{2n+1}$ . Intersecting each of the

quadrics  $Q_\lambda$  with  $H$ , one obtains a new pencil  $\overline{\mathcal{L}}$  in  $H \simeq \mathbb{P}^{2n}$ . This pencil  $\overline{\mathcal{L}}$  is generic in the sense it contains precisely  $2n + 1$  singular quadrics all of which are simple quadric cones. As we have seen in Section 1.1, classical intersection theory implies that the number of  $(n - 1)$ -planes  $\mathbb{P}X$  contained in the base locus of  $\overline{\mathcal{L}}$  is  $2^{2n}$ . By definition, these also lie in the base locus of  $\mathcal{L}$ . Furthermore,  $T_{\mathbb{P}X}B = \text{Span}(\mathbb{P}X, p_i)$  is an  $n$ -plane contained in  $Q_{\lambda_i}$ . For any such  $\mathbb{P}X$ ,

$$\mathbb{P}X +_G \mathbb{P}X = (P_i).$$

**Lemma 1.15.** For a generic pencil  $\mathcal{L}$ ,  $\dim(T_{\mathbb{P}X}B) \leq n$ .

**Proof:** Suppose without loss of generality  $Q_1, Q_2$  are non-degenerate. Since  $\dim(X) = n$ , it follows that  $\dim(X^{\perp_{Q_i}}) = n + 2$  for  $i = 1, 2$ . Suppose for a contradiction that  $\dim(T_{\mathbb{P}X}B) \geq n + 1$ . Then

$$X^{\perp_{Q_1}} = X^{\perp_{Q_2}} =: H.$$

Since the cone points span the entire  $\mathbb{P}(U)$ , there exists a cone point  $[v_\lambda]$  of a singular quadric  $Q_\lambda \in \mathcal{L}$  such that  $v_\lambda \notin H$ . Since  $Q_\lambda$  descends to a quadratic form on the 2-dimensional vector space  $H/X$ , there exists a vector  $v \in H \setminus X$  such that  $Q_\lambda(v) = 0$ . Now,

$$\text{Span}\{X, v, v_\lambda\} \subset U$$

is an  $(n + 2)$ -dimensional isotropic subspace with respect to  $Q_\lambda$ . However, since  $Q_\lambda$  is a simple quadric cone, its maximal isotropic subspace has dimension  $n + 1$ .  $\square$

We will prove Theorem 1.10 by proving the following three Propositions.

**Proposition 1.16.**  $\text{Div}(C)$  acts transitively on  $F \dot{\cup} F'$ .

**Proposition 1.17.** The principal divisors act trivially on  $F \dot{\cup} F'$ . Since  $[D_0]$  acts trivially, we now have a transitive action of  $H$  on  $F \dot{\cup} F'$ .

**Proposition 1.18.** If  $[D] \in H$  acts trivially, then  $[D] = 0$ .

Without loss of generality, we assume that  $k$  is algebraically closed. The following two lemmas proved in [7] are crucial in proving these propositions.

**Lemma 1.19.** ([7, Lemma 2.6]) Suppose  $\mathbb{P}X, \mathbb{P}X' \in F$  intersect at codimension  $r$ . There exists a unique effective divisor  $D$  of degree  $r$  such that

$$\mathbb{P}X + D = \mathbb{P}X' \text{ if } r \text{ is even, } \quad \mathbb{P}X + D = -\mathbb{P}X' \text{ if } r \text{ is odd.}$$

**Lemma 1.20.** ([7, Lemma 3.2]) Suppose  $[D] \in \text{Pic}(C)$  is effective with  $\dim H^0(\mathcal{O}_C[D]) \geq 2$ , where

$$H^0(\mathcal{O}_C[D]) = \{f \in k^s(C) \mid [D] + \text{div}(f) \geq 0\}.$$

Then  $[D] - [D_0]$  is also effective.

**Proof of Proposition 1.16:** It suffices to show the existence of an element  $D \in \text{Div}(C)$  sending  $-\mathbb{P}X$  to  $\mathbb{P}X'$  for both  $\mathbb{P}X, \mathbb{P}X' \in F$ . First suppose  $\mathbb{P}X$  satisfies the condition of 4c), namely  $T_{\mathbb{P}X}B$  is an  $n$ -plane and correspondingly  $\mathbb{P}X + \mathbb{P}X = (e)$ . We claim via induction on the codimension  $r$  of the intersection  $X' \cap X$  in  $X$ , that there is an element  $D \in \text{Div}(C)$  such that  $[D] + (-\mathbb{P}X) = \mathbb{P}X'$ . The base case  $r = 0$  is when  $\mathbb{P}X = \mathbb{P}X'$ , in which case  $[D] = (e)$  does the job. The case  $r = 1$  is covered by 4d(i). Suppose the claim is true for all  $\mathbb{P}X''$  intersecting  $\mathbb{P}X$  at codimension  $\leq r - 1$  and  $\text{codim}(\mathbb{P}X' \cap \mathbb{P}X) = r$ . Choose any  $\mathbb{P}X'' \in F$  intersecting  $\mathbb{P}X'$  at codimension 1 and  $\mathbb{P}X$  at  $r - 1$ . Denote by  $D'' \in \text{Div}(C)$  the element sending  $-\mathbb{P}X$  to  $\mathbb{P}X''$ . Consider

$$D' = (\mathbb{P}X' + \mathbb{P}X'') - D'' + (e).$$

From our definition of the action of  $H$  on  $F \dot{\cup} F'$ , we know that

$$-D'' + \mathbb{P}X = -(D'' + (-\mathbb{P}X)) = -\mathbb{P}X''.$$

Now  $(e)$  sends  $-\mathbb{P}X$  to  $\mathbb{P}X$ ,  $-D''$  sends  $\mathbb{P}X$  to  $-\mathbb{P}X''$ , and  $(\mathbb{P}X' + \mathbb{P}X'')$  sends  $-\mathbb{P}X''$  to  $\mathbb{P}X'$ . Therefore the composition  $D'$  sends  $-\mathbb{P}X$  to  $\mathbb{P}X'$  as desired.

Next, let  $\mathbb{P}X', \mathbb{P}X'' \in F$  be arbitrary. Let  $D', D''$  denote the elements in  $\text{Div}(C)$  sending  $-\mathbb{P}X$  to  $\mathbb{P}X', \mathbb{P}X''$  respectively. Consider

$$D = D' - (e) + D''.$$

Now  $D''$  sends  $-\mathbb{P}X''$  to  $\mathbb{P}X$ ,  $-(e)$  sends  $\mathbb{P}X$  to  $-\mathbb{P}X$ , and  $D'$  sends  $-\mathbb{P}X$  to  $\mathbb{P}X'$ . Note this also proves the existence part of Lemma 1.19.  $\square$

**Lemma 1.21.** If  $D \in \text{Div}(C)$  fixes some  $x_0 \in F \dot{\cup} F'$ , then  $D$  acts trivially.

**Proof:** This follows immediately from transitivity of the action.  $\square$

**Lemma 1.22.** If  $D, E$  are effective divisors of degree at most  $n$ , and  $D - E = \text{div}(f)$  is a principal divisor, then  $D - E$  acts trivially.

**Proof:** Applying Lemma 1.20 repeatedly to  $D$ , one obtains a unique effective divisor  $D_1$  with  $h^0(D_1) = 1$  and such that  $D$  and  $E$  are in the linear system  $D_1 + \frac{\deg(D) - \deg(D_1)}{2} D_0$ . Since  $\deg(D) \leq n$ ,  $H^0(\mathcal{O}_C(\frac{\deg(D) - \deg(D_1)}{2} D_0))$  consists of functions pulled back from  $\mathbb{P}^1$ . Hence  $D - E$  is a linear combination of divisors of the form  $(P) + (\bar{P})$  which acts trivially on  $F \dot{\cup} F'$  by construction.  $\square$

Let  $\infty$  denote a Weierstrass point of  $C$  defined over  $k^s$ .

**Lemma 1.23.** Suppose  $D = (P_1) + \cdots + (P_r) - r(\infty) \in \text{Div}(C)$  with  $P_i \neq \infty$  and  $r \leq n$ . If  $D$  is linearly equivalent to  $E = (Q_1) + \cdots + (Q_{r'}) - r'(\infty)$  with  $Q_i \neq \infty$  and  $r' \leq r$ , then  $x + D = x + E$  for all  $x \in F \dot{\cup} F'$ .

**Proof:** Apply Lemma 1.22 to the effective divisors  $(P_1) + \cdots + (P_r)$  and  $(Q_1) + \cdots + (Q_{r'}) + (r - r')(\infty)$ .  $\square$

Every divisor class  $[D] \in J = \underline{\text{Pic}}^0(C)$  can be represented by a divisor of the form  $(P_1) + \cdots + (P_r) - r(\infty)$  with  $r \leq n$ . Lemma 1.23 says that two different representations of  $[D]$  have the

same action on  $F \dot{\cup} F'$ . Since  $\deg(D)$  is even, it sends  $F$  to  $F$ . Therefore we have a morphism of varieties

$$\alpha : J \rightarrow \text{Aut}(F).$$

The image of  $\alpha$  lies in a commutative subvariety of the identity component of  $\text{Aut}(F)$ . Since  $J$  is complete and  $\alpha([0]) = \text{id}$ , rigidity ([12, pp.40–41]) implies that  $\alpha$  is a group homomorphism.

**Proof of Proposition 1.17:** Let  $\beta : \text{Div}^0(C) \rightarrow \text{Aut}(F)$  denote the action map. To show the principal divisors act trivially, it suffices to show  $\beta$  factors through  $\alpha : J \rightarrow \text{Aut}(F)$ . Both are group homomorphisms, therefore it suffices to check

$$\beta((c) - (c')) = \alpha([(c) - (c')])$$

for any  $c, c' \in C$ . For any  $\mathbb{P}X \in F$ ,

$$\begin{aligned} \alpha([(c) - (c')])(\mathbb{P}X) &= \mathbb{P}X + (c) - (\infty) + (\overline{c'}) - (\infty) \\ &= \mathbb{P}X + (c) - (c') \\ &= \beta((c) - (c'))(\mathbb{P}X). \quad \square \end{aligned}$$

Given two elements  $x = \pm \mathbb{P}X, x' = \pm \mathbb{P}X'$  of  $F \dot{\cup} F'$ , we define their **intersection codimension** as the intersection codimension of  $\mathbb{P}X, \mathbb{P}X'$  and write

$$\text{codim}(x, x') = \text{codim}(\mathbb{P}X, \mathbb{P}X').$$

In this notation, Lemma 1.19 can be stated as follows:

**Lemma 1.24.** Suppose  $x, x' \in F$  or  $x, x' \in F'$ . Then there exists a unique effective divisor  $D$  of degree  $r = \text{codim}(x, x')$  such that

$$x + D = (-1)^r x'.$$

**Lemma 1.25.** Suppose  $D$  is an effective divisor of degree  $r \leq n, r \geq 1$ , then there exists an

$x \in F$  such that

$$\text{codim}(x, x + D) \equiv r \pmod{2}.$$

There is also an  $x \in F'$  satisfying the same condition.

**Proof:** Suppose for a contradiction that for all  $x \in F$ ,

$$\text{codim}(x, x + D) \equiv r - 1 \pmod{2}. \quad (1.5)$$

Consider the following variety

$$\Sigma = \{(x, c_1, \dots, c_{r-1}) \mid x \in F, c_i \in C, x + D = -x + (c_1) + \dots + (c_{r-1})\} \subset F \times \text{Sym}^{r-1}(C).$$

When  $r = 1$ ,  $\Sigma = \{x \in F \mid x + D = -x\}$ . It is clear from the definition that  $\Sigma$  is closed. Denote the two projections to  $F$  and  $\text{Sym}^{r-1}(C)$  by  $\pi_1, \pi_2$  respectively. For any  $x \in F$ ,

$$\text{codim}(x, x + D) =: r' \leq r.$$

By Lemma 1.24, there exists an effective divisor  $D'$  of degree  $r'$  such that

$$x + D = (-1)^{r-r'}(x + D').$$

Assumption (1.5) says  $r - r'$  is odd for all  $x$ . Therefore, replacing  $D'$  by  $D' + (r - 1 - r')(\infty)$ , we see that  $\pi_1$  is surjective. Since  $\dim(F) \geq n$  and  $\dim(\text{Sym}^{r-1}(C)) = r - 1 < n$ , there exists a fiber of  $\pi_2$  of positive dimension. In other words, there exists a divisor  $\tilde{D}$  of odd degree such that for infinitely many  $x \in F$ ,

$$x + \tilde{D} = -x. \quad (1.6)$$

Let  $D_1$  be a divisor such that  $2D_1 - (\infty)$  is linearly equivalent to  $\tilde{D}$ . Since we have shown

that the principal divisors act trivially, (1.6) implies that for infinitely many  $x \in F$ ,

$$(x + D_1) = -(x + D_1) + (\infty).$$

Hence for infinitely many  $\mathbb{P}X \in F$ ,

$$\mathbb{P}X = \tau(\infty)\mathbb{P}X.$$

However, we have seen in condition 4c) that there are only  $2^{2n}$  such  $\mathbb{P}X$ . Contradiction.

The statement for  $F'$  follows from the same argument, which is the main reason why we have used  $x$  to denote an element of  $F$  instead of the usual  $\mathbb{P}X$ .  $\square$

**Proof of Proposition 1.18:** Suppose  $D = (P_1) + \cdots + (P_r) - r(\infty)$  acts trivially on  $F$  with  $r \leq n$  minimal and  $P_i \neq \infty$ .

Suppose first that  $r = 2r'$  is even. Then for all  $\mathbb{P}X \in F$ ,

$$\mathbb{P}X + (P_1) + \cdots + (P_{r'}) = \mathbb{P}X + (\overline{P}_{r'+1}) + \cdots + (\overline{P}_r). \quad (1.7)$$

By lemma 1.25, there exists  $\mathbb{P}X_0 \in F$  such that

$$\text{codim}(\mathbb{P}X_0, \mathbb{P}X_0 + (P_1) + \cdots + (P_{r'})) = r'' \equiv r' \pmod{2}.$$

Therefore, there exists points  $Q_1, \dots, Q_{r''} \in C$  such that

$$\mathbb{P}X_0 + (P_1) + \cdots + (P_{r'}) = \mathbb{P}X_0 + (Q_1) + \cdots + (Q_{r''}).$$

Lemma 1.21 says if a divisor fixes one  $\mathbb{P}X_0 \in F$ , then it acts trivially on  $F$ . Hence the divisor

$$(Q_1) + \cdots + (Q_{r''}) + (P_{r'+1}) + \cdots + (P_r) - (r'' + r')(\infty)$$

acts trivially on  $F$ . Minimality of  $r$  forces  $r'' = r'$ . That is,

$$\text{codim}(\mathbb{P}X_0, \mathbb{P}X_0 + (P_1) + \cdots + (P_{r'})) = r'.$$

Lemma 1.19 then implies

$$(P_1) + \cdots + (P_{r'}) = (\overline{P}_{r'+1}) + \cdots + (\overline{P}_r)$$

as effective divisors of degree  $r'$ . Therefore  $D = 0$ .

Suppose now  $r = 2r' + 1$  is odd. Then for all  $\mathbb{P}X \in F$ ,

$$\mathbb{P}X + (P_1) + \cdots + (P_{r'+1}) = \mathbb{P}X + (\overline{P}_{r'+2}) + \cdots + (\overline{P}_r) + (\infty) \quad (1.8)$$

Argue just like the even case, we see that minimality of  $r$  implies that for some  $\mathbb{P}X_0 \in F$ ,

$$\text{codim}(\mathbb{P}X_0, \mathbb{P}X_0 + (P_1) + \cdots + (P_{r'+1})) = r' + 1.$$

Then Lemma 1.19 implies

$$(P_1) + \cdots + (P_{r'+1}) = (\overline{P}_{r'+2}) + \cdots + (\overline{P}_r) + (\infty)$$

as effective divisors of degree  $r' + 1$ . Therefore  $D = 0$ . □

We have completed the proofs of Propositions 1.16, 1.17, and 1.18. Before moving on to state the main theorem, we describe a stronger form of Lemma 1.25 for completeness.

Lemma 1.20 implies that if  $(P_1) + \cdots + (P_r) - r(\infty)$  and  $(Q_1) + \cdots + (Q_r) - r(\infty)$ , with  $r \leq n$ , are two distinct divisors representing the same divisor class  $[D] \in J$ , then  $[D]$  can also be represented by a divisor of the form  $(R_1) + \cdots + (R_{r-2}) - (r-2)(\infty)$ . Therefore if  $r$  is minimal



among all such representations of  $[D]$ , there is a unique effective divisor  $D'$  of degree  $r$  such that

$$[D' - r(\infty)] = [D].$$

We call  $D'$  the  $\infty$ -**minimal form** of  $[D]$ .

**Corollary 1.26.** Let  $D'$  be the  $\infty$ -minimal form of a nonzero divisor class  $[D]$ . Then there exists an  $x \in F$  such that

$$\text{codim}(x, x + D') = \deg(D').$$

There is also an  $x \in F'$  satisfying the same condition.

**Proof:** Let  $r$  denote the degree of  $D'$ . Lemma 1.25 allows us to pick an  $x \in F$  such that

$$\text{codim}(x, x + D') =: r' \equiv r \pmod{2}.$$

By Lemma 1.24, there exists an effective divisor  $D''$  of degree  $r'$  such that  $x + D' = x + D''$ . Hence  $D' - D''$  fixes  $x$  and by Lemma 1.21,  $D' - D''$  acts trivially on  $F$ . By Proposition 1.18,  $D'$  is linearly equivalent to  $D''$ . Since  $D'$  is the  $\infty$ -minimal form of  $[D]$ , we see that  $r' = r$ .

The statement for  $F'$  follows from the same argument. □

We now state our theorem in its completion.

**Theorem 1.27.** Let  $G$  be the disconnected variety

$$G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F',$$

where  $F'$  is a copy of  $F$ . There is a commutative algebraic group structure  $+_G$  on  $G$  over  $k$  such that,

1.  $G^0 = \underline{\text{Pic}}^0(C)$  with component group  $G/G^0 \simeq \mathbb{Z}/4\mathbb{Z}$ ,
2.  $F'$  is isomorphic to  $F$  as varieties via the inversion map  $-1_G$ ,

3. the group law extends that on  $H = \underline{\text{Pic}}(C)/\mathbb{Z}D_0 \simeq \underline{\text{Pic}}^0(C) \dot{\cup} \underline{\text{Pic}}^1(C)$  where  $D_0$  is the hyperelliptic class,
4. the group law defines a simply-transitive action of  $H$  on  $F \dot{\cup} F'$  extending the following action of  $C$  :

$$\mathbb{P}X + (c) = -\tau(c)\mathbb{P}X, \quad -\mathbb{P}X + (c) = \tau(\bar{c})\mathbb{P}X,$$

with respect to which  $x +_G x'$ , for  $x, x' \in F \dot{\cup} F'$ , is the unique divisor class sending  $-x$  to  $x'$ .

**Proof:** The only thing left to check is the associativity, which amounts to the following four:

$$\begin{aligned} [D_1] +_G ([D_2] +_G [D_3]) &= ([D_1] +_G [D_2]) +_G [D_3] \\ x +_G ([D_2] +_G [D_3]) &= (x +_G [D_2]) +_G [D_3] \\ x +_G (x' +_G [D_3]) &= (x +_G x') +_G [D_3] \\ x +_G (x' +_G x'') &= (x +_G x') +_G x'', \end{aligned}$$

for  $[D_1], [D_2], [D_3] \in H$  and  $x, x', x'' \in F \dot{\cup} F'$ .

The first one is associativity of the group law on  $H$ . The second follows from the definition of the action of  $H$ . The third follows as both sides send  $-x$  to  $x' + [D_3]$ . For the fourth one, denote the two sides by  $x_L$  and  $x_R$  and add  $x'$  to both sides. The third associativity tells us  $x' +_G x_L = (x' +_G x) +_G (x' +_G x'')$  and likewise,  $x_R +_G x' = (x +_G x') +_G (x'' +_G x')$ . Commutativity of  $+_G$  implies these two elements of  $\underline{\text{Pic}}^0(C)$  are equal. Therefore  $x_L = x_R$  is the image of  $-x'$ .  $\square$

**Corollary 1.28.** The class  $[F] \in H^1(k, J)$  is 4-torsion, twice of which is  $[\underline{\text{Pic}}^1(C)]$ . One can lift  $[F]$  to a torsor of  $J[4]$  by taking

$$F[4] := \{\mathbb{P}X \in F \mid \mathbb{P}X +_G \mathbb{P}X +_G \mathbb{P}X +_G \mathbb{P}X = 0\}.$$

**Proof:** With our convention of Galois cohomology, we need to show  $F(k^s)$  is nonempty. Let  $P$  be a Weierstrass point, it is defined over  $k^s$  because  $f(x)$  splits over  $k^s$ . We saw there are

precisely  $2^{2n}$  elements of  $F(k^s)$  satisfying  $\mathbb{P}X +_G \mathbb{P}X = (P)$ . They correspond to  $(n-1)$ -planes contained in the base locus of a generic pencil in  $\mathbb{P}^{2n}$ . Theorem 1.3 says they are in fact all defined over  $k^s$ .  $\square$

When  $C$  admits a rational divisor class of odd degree,  $\underline{\text{Pic}}^1(C)(k) \neq \emptyset$ . In this case,  $[F]$  is 2-torsion and it lifts to a torsor of  $J[2]$ . See Section 2.1 for more about lifting torsors of  $J$  of finite order.

### 1.2.2 Torsor for $J[2]$

Fix a  $2n+2$  dimensional quadratic space  $(U, Q)$  of discriminant 1. There are two rulings of projective  $n$ -planes contained in the quadric defined by  $Q$ . The two rulings are defined over  $k(\sqrt{\text{disc}(Q)})$  and are acted on by the group  $\text{PO}(U, Q)$ , each with stabilizer  $\text{PSO}(U, Q) =: \text{PSO}_{2n+2}$ . Fix one such ruling  $Y_0$  defined over  $k$ . If  $Q$  is split, we also abuse notation to use  $Y_0$  to denote an isotropic  $k$ -rational (linear)  $n+1$  plane. If  $Y$  is any subspace defined over  $k^s$ , we write  $Y \sim Y_0$  if  $Y$  is isotropic of dimension  $n+1$  and if their intersection codimension in either one of them is even. This is equivalent to saying  $\mathbb{P}Y$  and  $\mathbb{P}Y_0$  lie in the same ruling, as projective  $n$ -planes contained in the quadric defined by  $Q$ .

Let  $f(x) \in k[x]$  be any separable monic polynomial of degree  $2n+2$ , we want to study a certain simply-transitive action of  $\text{PSO}_{2n+2}$ . Consider the following three  $k$ -schemes,

$$\begin{aligned} V_f &= \{T : U \rightarrow U \mid T^* = T, \text{ characteristic polynomial of } T \text{ is } f\} \\ W_f &= \{(T, X) \in V_f \times \text{Gr}(n, U) \mid \text{Span}\{X, TX\} \sim Y_0\} \\ W_T &= \{X \mid (T, X) \in W_f\} \text{ for } T \in V_f(k) \end{aligned}$$

Here  $\text{Span}\{X, TX\} \sim Y_0$  means that  $\text{Span}\{X, TX\}$  is an  $(n+1)$ -plane isotropic with respect to  $Q$  lying in the same ruling as  $Y_0$ . We will show in Proposition 2.18 that  $W_T$  this recovers the lift of  $[F]$  mentioned at the end of the previous section.

Since  $\text{PSO}_{2n+2}$  preserves the rulings, if  $Y \sim Y_0$ , then  $gY \sim Y_0$  for any  $g \in \text{PSO}_{2n+2}$ . Therefore,

$\mathrm{PSO}_{2n+2}$  acts on  $W_f$  via

$$g.(T, X) = (gTg^{-1}, gX).$$

**Proposition 1.29.** If  $f(x)$  splits completely over  $k$  and  $k = k^2$ , for example  $k = k^s$ , then  $\mathrm{PSO}_{2n+2}(k)$  acts transitively on  $V_f(k)$ . For general  $k$ , suppose  $T \in V_f(k')$  is defined over some field  $k'$  containing  $k$ . Then its stabilizer scheme  $\mathrm{Stab}(T)$  is isomorphic to  $(\mathrm{Res}_{L'/k'} \mu_2)_{N=1} / \mu_2$  as group schemes over  $k'$  where  $L' = k'[x]/f(x)$ .

**Proof:** Just as in the proof of Proposition 1.1, for any  $T \in V_f(k')$ ,

$$\begin{aligned} \mathrm{Stab}_{GL(U_{k'})}(T) &\simeq \mathrm{Res}_{L'/k'} \mathbb{G}_m, \\ \mathrm{Stab}_{O(U_{k'}, Q)}(T) &\simeq \mathrm{Res}_{L'/k'} \mu_2, \\ \mathrm{Stab}_{SO(U_{k'}, Q)}(T) &\simeq (\mathrm{Res}_{L'/k'} \mu_2)_{N=1}, \\ \mathrm{Stab}_{PSO(U_{k'}, Q)}(T) &\simeq (\mathrm{Res}_{L'/k'} \mu_2)_{N=1} / \mu_2. \end{aligned}$$

Suppose now  $f(x)$  splits completely in  $k$  and  $k = k^2$ . Suppose  $T_1, T \in V_f(k)$ . There exists  $g \in GL(U)(k)$  such that  $T_1 = gTg^{-1}$ . Since  $T_1$  and  $T$  are both self-adjoint,  $g^*g$  centralizes  $T$  and hence lies in  $(k[T]/f(T))^\times$  which is a product of  $k^\times$  since  $f$  splits. Since  $k = k^2$ , there exists  $h \in (k[T]/f(T))^\times$  such that  $g^*g = h^2$ . Then  $gh^{-1}$  is an element of  $O(U, Q)(k)$  conjugating  $T$  to  $T_1$ . Multiplying the  $h$  by  $(-1, 1, \dots, 1) \in (k[T]/f(T))^\times$  if necessary, we may assume  $gh^{-1} \in \mathrm{SO}(U, Q)(k)$ . Its image in  $\mathrm{PSO}(U, Q)(k)$  does the job.  $\square$

**Lemma 1.30.** If  $Q$  is split, then both  $V_f(k)$  and  $W_f(k)$  are nonempty. Furthermore, there exists  $(T_0, X_0) \in W_f(k)$  with trivial stabilizer in  $\mathrm{PSO}_{2n+2}(k^s)$ .

**Proof:** Consider the  $2n + 2$  dimensional étale  $k$ -algebra  $L = k[x]/f(x) = k[\beta]$ . On  $L$  there is the following bilinear form

$$\langle \lambda, \mu \rangle = \mathrm{Tr}(\lambda\mu/f'(\beta)) = \text{coefficient of } \beta^{2n+1} \text{ in } \lambda\mu.$$

This form defines a split quadratic form since  $Y = \mathrm{Span}_k\{1, \beta, \dots, \beta^n\}$  is a rational maximal

isotropic subspace. Hence there exists an isometry from  $(L, <, >)$  to  $(U, Q)$  defined over  $k$ . Via this identification, the operator  $\cdot\beta$  on  $L$  transforms into a self-adjoint operator  $T_0$  on  $U$ . Denote by  $X_0$  the image of  $X = \text{Span}_k\{1, \beta, \dots, \beta^{n-1}\}$  under this isometry. Since  $(\cdot\beta, X)$  has trivial stabilizer in  $\text{PSO}(L, <, >)(k^s)$ , the corresponding element  $(T_0, X_0) \in W_f(k)$  has trivial stabilizer in  $\text{PSO}_{2n+2}(k^s)$ .  $\square$

**Theorem 1.31.** Suppose  $k$  is separably closed. Then  $\text{PSO}(V, Q)(k)$  acts simply-transitively on  $W_f(k)$ .

**Proof:** Suppose  $k$  is separably closed. Proposition 1.29 shows it suffices to prove that for the  $T_0 \in V_f(k)$  obtained in the above lemma,  $\text{Stab}(T_0)(k)$  acts simply-transitively on  $W_{T_0}(k)$ . Since  $(T_0, X_0)$  has trivial stabilizer, it suffices to show they have the same size. As a consequence of Proposition 2.18, for any  $k$ ,  $W_T(k^s) = F_T[2]_\infty(k^s)$  has  $2^{2n}$  elements for any  $T$ . Hence we are done because,

$$2^{2n} = |(\text{Res}_{L/k}\mu_2/\mu_2)_{N=1}(k)| = |\text{Stab}(T_0)(k)| \leq |W_{T_0}(k)| \leq |W_{T_0}(k^s)| = 2^{2n}. \quad \square$$

**Theorem 1.32.** Suppose  $W_f(k)$  is non-empty. Then  $\text{PSO}_{2n+2}(k')$  acts simply-transitively on  $W_f(k')$  for any field  $k'$  containing  $k$ .

**Proof:** Same descent argument as in the proof of Theorem 1.4.  $\square$

**Corollary 1.33.** For any  $T \in V_f(k)$ ,  $W_T(k')$  is a principal homogeneous space for  $J[2](k')$  for any field  $k'$  containing  $k$ .

**Proof:** Same as the proof of Corollary 1.5, except now as group schemes over  $k$ ,

$$\text{Stab}(T) \simeq (\text{Res}_{L/k}\mu_2)_{N=1}/\mu_2 \simeq J[2]. \quad \square \tag{1.9}$$

**Remark 1.34.** One can write down an explicit formula for (1.9). The method is the same as the odd case in Remark 1.6. Denote the roots of  $f(x)$  over  $k^s$  by  $\alpha_1, \dots, \alpha_{2n+2}$ , and for each  $i$ ,

define  $h_i(x) = f(x)/(x - \alpha_i)$ . Then on the level of  $k^s$ -points, (1.9) is given by sending

$$\sum n_i(\alpha_i) - \frac{\sum n_i}{2}((\infty) + (\infty')), \quad \sum n_i \text{ even},$$

to the image in  $\mathrm{PSO}_{2n+2}(k^s)$  of

$$\prod \left(1 - 2 \frac{h_i(T)}{h_i(\alpha_i)}\right)^{n_i} = 1 - 2 \sum n_i \frac{h_i(T)}{h_i(\alpha_i)}. \quad (1.10)$$

Note as a polynomial of degree at most  $2n + 1$ ,  $\sum_{i=1}^{2n+2} h_i(x)/h_i(\alpha_i)$  takes the value 1 when  $x = \alpha_1, \dots, \alpha_{2n+2}$ , hence it must be the constant polynomial 1. Thus,

$$\prod_{i=1}^{2n+2} \left(1 - 2 \frac{h_i(T)}{h_i(\alpha_i)}\right) = -1 = 1 \text{ in } \mathrm{PSO}_{2n+2}.$$

We will see in Proposition 2.7 and Proposition 2.21 that  $1 - 2 \frac{h_i(T)}{h_i(\alpha_i)}$  is a reflection, hence has determinant  $-1$ . The assumption that  $\sum n_i$  is even ensures that the product in (1.10) lies in  $\mathrm{SO}$ .

### 1.3 A specialization argument

In this section, we deal with the more technical details that we pointed out in the previous sections. Suppose  $\mathcal{L}$  is a rational generic pencil of quadrics in  $\mathbb{P}^{2n+1}$  and let  $C$  denote its associated hyperelliptic curve parameterizing rulings in the pencil. Let  $B$  denote the base locus of the pencil and let  $F$  denote the variety of  $(n - 1)$ -planes contained in  $B$ .

The crucial geometric input in Section 1.2 is the map  $\tau : C \times F \rightarrow F$ . Recall that for any  $(c, \mathbb{P}X) \in C \times F$ , there exists a unique  $n$ -plane  $\mathbb{P}Y$  containing  $\mathbb{P}X$  in the ruling of the quadric defined by  $c$ . The intersection of  $\mathbb{P}Y$  with  $B$  is a union of two (possibly equal)  $n - 1$  planes one of which is  $\mathbb{P}X$ . We defined  $\tau(c, X)$  to be the other  $n - 1$  plane.

**Lemma 1.35.** The map  $\tau : C \times F \rightarrow F$  is a morphism of varieties.

**Proof:** Let  $\tilde{F}$  denote the following closed subvariety of  $\mathcal{L} \times \mathbb{G}r(n, \mathbb{P}U)$ ,

$$\tilde{F} = \{(Q, \mathbb{P}Y) | \mathbb{P}Y \simeq \mathbb{P}^n, Y \subseteq Q, Q \in \mathcal{L}\}.$$

The hyperelliptic curve  $C$  can be viewed as the Stein factorization of the projection map  $\tilde{F} \rightarrow \mathcal{L}$ . Denote by  $\epsilon : \tilde{F} \rightarrow C$  the corresponding map. Consider the closed subvariety  $\Sigma$  of  $(C \times F) \times_C \tilde{F}$  consisting of quadruples  $(c, \mathbb{P}X, Q, \mathbb{P}Y)$  where  $\mathbb{P}X \subset \mathbb{P}Y$  and  $\epsilon(Q, \mathbb{P}Y) = c$ . We claim that the following composite map

$$\gamma : \Sigma \hookrightarrow (C \times F) \times_C \tilde{F} \rightarrow C \times F$$

is an isomorphism of varieties. The uniqueness of the  $n$ -plane  $\mathbb{P}Y$  that lies in a fixed ruling of a quadric and contains a given  $n - 1$  plane implies that  $\gamma$  is bijective on points. It is also separable because the corresponding field extension is at most degree 2 and the characteristic of  $k$  is assumed to be not 2. Therefore by Zariski's Main Theorem,  $\gamma$  is an isomorphism.

Let  $\Sigma' \subset F \times \tilde{F}$  denote the image of  $\Sigma$  in  $(C \times F) \times_C \tilde{F}$ . By definition,  $\Sigma'$  consists of triples  $(\mathbb{P}X, Q, \mathbb{P}Y)$  such that  $\mathbb{P}X \subset \mathbb{P}Y \subset Q$ . Let  $r$  denote the map  $\Sigma' \rightarrow F$  defined by

$$\mathbb{P}Y \cap B = \mathbb{P}X \cup r(\mathbb{P}X, Q, \mathbb{P}Y).$$

By writing down explicit equations, we see that  $r$  is a morphism. Finally, the map  $\tau$  is the following composition of morphisms:

$$C \times F \xrightarrow{\gamma^{-1}} \Sigma \rightarrow \Sigma' \xrightarrow{r} F.$$

Therefore  $\tau$  is a morphism. □

Let  $G$  denote the disconnected subvariety

$$G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F',$$

where  $F'$  is a copy of  $F$ . In Section 1.2.1, we defined a group structure on  $G(k^s)$ . We now prove that  $+_G : G \times G \rightarrow G$  is a morphism of varieties. Indeed this follows formally from the fact that  $+_G$  is  $J(k^s)$ -equivariant, separable descent, and the following result.

**Theorem 1.36.** Suppose  $k$  is separably closed. Then the following morphism is an isomorphism.

$$\begin{aligned} \iota : J \times F &\rightarrow F \times F \\ ([D], \mathbb{P}X) &\mapsto ([D] + \mathbb{P}X, \mathbb{P}X). \end{aligned}$$

In other words,  $F$  is a torsor of  $J$  in the conventional sense.<sup>1</sup>

Theorem 1.36 implies that  $J$  is isomorphic to every component of  $G$  over  $k^s$ . In particular, there exists an isomorphism  $G \simeq J \times \mathbb{Z}/4\mathbb{Z}$  over  $k^s$  such that  $+_G$  becomes the usual addition on  $J \times \mathbb{Z}/4\mathbb{Z}$ .

We assume for the rest of this section that  $k$  is separably closed and prove Theorem 1.36. From Section 1.2.1 we know that  $\iota$  is bijective on the level of points. Zariski's Main Theorem then implies it is a finite morphism. The only possible issue here is inseparability. Hence, Theorem 1.36 holds automatically when the characteristic of  $k$  is 0. Moreover, if one chases through the proof of Lemma 1.19 ([7, Lemma 2.6]), one can show that  $\iota$  is separable if the characteristic of  $k$  is larger than  $n$ . We will prove  $\iota$  is an isomorphism for all characteristics using a specialization argument from characteristic 0.

Let  $S$  be a reduced and normal scheme over  $\mathbb{Z}[1/2]$  and let  $\mathcal{Q}_1, \mathcal{Q}_2$  be a degenerate quadric and a non-degenerate quadric in  $\mathbb{P}_S^{2n+1}$  over  $S$  respectively. The pencil  $\mathcal{L}$ , its associated hyperelliptic curve  $\mathcal{C}$  and the corresponding Fano variety  $\mathcal{F}$  of  $n-1$  planes in the base locus can all be defined over  $S$ . By removing a closed subscheme of  $S$ , we assume that  $\mathcal{L}$  is a generic pencil fiberwise over  $S$  and hence  $\mathcal{C}$  is smooth over  $S$ . Since  $\mathcal{Q}_1$  is degenerate, the map  $\mathcal{C} \rightarrow S$  has a section. Let  $\mathcal{J}$  denote the relative Jacobian scheme. Since  $\mathcal{C} \rightarrow S$  has a section, no sheafification is needed in the definition of  $\mathcal{J}$ .

---

<sup>1</sup>I would like to especially thank Bjorn Poonen for pointing out this problem and to thank him and Anand Patel for suggesting the following solution.



Using the section  $S \rightarrow \mathcal{C}$  and the morphism  $\tau : \mathcal{C} \times_S \mathcal{F} \rightarrow \mathcal{F}$ , we get a morphism

$$\alpha : \mathcal{C} \simeq \mathrm{Sym}^1(\mathcal{C}) \rightarrow \underline{\mathrm{Aut}}_S(\mathcal{F})^0.$$

Lemma 1.9 allows us to extend  $\alpha$  to  $\mathrm{Sym}^n(\mathcal{C})$ . Since  $\mathrm{Sym}^n(\mathcal{C})$  is birational to  $\mathcal{J}$  using the section  $S \rightarrow \mathcal{C}$ , we get a rational map  $\alpha : \mathcal{J} \dashrightarrow \underline{\mathrm{Aut}}_S(\mathcal{F})^0$ . Since  $\mathcal{J}$  is smooth over  $S$ , the following properness result about  $\underline{\mathrm{Aut}}_S(\mathcal{F})^0$  allows us to extend  $\alpha$  to a morphism on  $\mathcal{J}$ .

**Lemma 1.37.** The group scheme  $\underline{\mathrm{Aut}}_S(\mathcal{F})^0$  is proper over  $S$ .

**Proof:** Over any geometric point  $s \in S$ , the Fano variety  $\mathcal{F}_s$  is an abelian variety. Indeed it is shown to be isomorphic to  $\mathcal{J}_s$  in [6]. We only need to know it is an abelian variety here. Therefore  $\underline{\mathrm{Aut}}_S(\mathcal{F})^0$  is faithfully flat over  $S$  with proper geometric fibers, and hence is proper over  $S$  by EGA IV.15.7.10.  $\square$

The upshot of extending  $\alpha$  to  $\mathcal{J}$  is that we now have the action morphism  $\mathcal{J} \times_S \mathcal{F} \rightarrow \mathcal{F}$  defined over  $S$ . Denote by  $\iota_S$  the morphism

$$\iota_S : \mathcal{J} \times_S \mathcal{F} \rightarrow \mathcal{F} \times_S \mathcal{F}.$$

We know  $\iota_S$  is an isomorphism on the generic fiber of  $S$  because the residue field at the generic fiber has characteristic 0. Moreover  $\iota_S$  is a bijection on the level of points, hence quasi-finite. The source  $\mathcal{J} \times_S \mathcal{F}$  is projective over  $S$ . The target  $\mathcal{F} \times_S \mathcal{F}$  is smooth over  $S$  and hence is reduced and normal. Therefore by Zariski's Main Theorem ([10, Corollary 11.4]),  $\iota_S$  is an isomorphism. The specialization of  $\iota_S$  to any geometric point of  $S$  is also an isomorphism.

To complete the proof of Theorem 1.36, it remains to show the existence of the above families over some scheme  $S$  such that for some geometric point  $s$  of  $S$ ,  $k(s) = k$ . For this we can take  $\mathcal{Q}_1, \mathcal{Q}_2$  to be the universal family and take  $S$  to be an open subscheme of  $\mathrm{Spec}\mathbb{Z}[1/2][x_1, \dots, x_N]$  where the indeterminates  $x_1, \dots, x_N$  correspond to the coordinates of the two quadrics.  $\square$

## 1.4 Odd dimension, regular case

We return to the case when  $U$  has dimension  $2n + 1$  and study a case more general than the nonsingular case treated in Section 1.1. Let  $Q$  be a non-degenerate quadratic form on  $U$  and let  $T$  be a self-adjoint operator on  $U$  with characteristic polynomial  $f_T$  splitting completely over  $k^s$ . We impose the condition that  $T$  is **regular** meaning that its minimal polynomial coincide with its characteristic polynomial. We want to study the set of  $n$ -planes  $X$  such that  $X \subset X^\perp, TX \subset X^\perp$ . As in Section 1.1, it is more convenient to let  $T$  vary as well.

Let  $f$  be a monic polynomial of degree  $2n + 1$  splitting completely over  $k^s$ . We define the  $k$ -scheme,

$$V_f = \{T : U \rightarrow U \mid T \text{ is self-adjoint and regular with characteristic polynomial } f(x)\}.$$

Note here regularity means there is no linear relations between  $1, T, \dots, T^{2n}$ . For every field  $k'$  containing  $k$ , and every  $T \in V_f(k')$ , let  $W_T(k')$  denote the set of (linear)  $n$ -dimensional  $k'$ -subspaces  $X$  of  $U \otimes k'$  such that  $X \subset X^\perp, TX \subset X^\perp$ . As before, we define

$$W_f(k') = \{(T, X) \mid T \in V_f(k'), X \in W_T(k')\}.$$

There is a Galois invariant action of  $\text{PO}(U, Q) = O(U, Q)/(\pm 1)$  on  $W_f$  :

$$g.(T, X) = (gTg^{-1}, gX).$$

Let  $K$  be either the separable closure or algebraic closure of  $k$ , and suppose  $f(x)$  factors as  $f(x) = \prod_{i=1}^{r+1} (x - \alpha_i)^{m_i}$  for  $\alpha_i \in K$ . In fact, we only need  $K$  to be a field over which  $f$  splits completely and that  $K = K^2$ ; but since we will not use the result in any case other than  $K = k^s, k^s$ , we will assume for the convenience of the reader that  $K$  is  $k^s$  or  $k^s$ . For any  $T \in V_f(K)$ , one can decompose  $U \otimes K$  into generalized  $T$ -eigenspaces. Namely,  $U \otimes K = \bigoplus_{i=1}^{r+1} U_{i,T}$  where each  $U_{i,T} \subset_K U$  is an  $m_i$ -dimensional  $K$ -subspace of  $U \otimes K$ . For any self-adjoint  $T$ , its generalized

eigenspaces are pairwise orthogonal with respect to  $Q$ . Therefore  $Q$  restricts to non-degenerate quadratic forms on each  $U_{i,T}$ . For any  $X \in W_T(K)$ ,  $X \cap U_{i,T}$  is isotropic and therefore has dimension at most  $m_i/2$ . For any sequence of integers  $d_1, \dots, d_{r+1}$  such that  $0 \leq d_i \leq m_i/2$ , for any intermediate field  $k'$  between  $k$  and  $K$ , and for any  $T \in V_f(k')$ , we define

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(k') = \{X \in W_T(k') \mid \dim(\text{maximal } T\text{-stable subspace of } (X \otimes K) \cap U_{i,T}) = d_i\},$$

$$W_{\{d_1, \dots, d_{r+1}\}}^f(k') = \{(T, X) \mid T \in V_f(k'), X \in L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(k')\}.$$

Note when  $f$  has no repeated roots, all  $m_i$  equal to 1, all  $d_i$  are 0 and  $L_{\{0, \dots, 0\}}^{f,T}(k')$ ,  $W_{\{0, \dots, 0\}}^f(k')$  recover  $W_T(k')$ ,  $W_f(k')$  respectively. Observe also that eigenvectors of  $T$  corresponding to eigenvalues of multiplicity 1 are never isotropic, since they are orthogonal to all the other generalized eigenspaces. If  $X \in L_{\{0, \dots, 0\}}^{f,T}(k')$ , then  $X$  contains no non-zero stable  $T$ -subspace. The main theorem we are heading towards is the following:

**Theorem 1.38.**  $|L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)| = 2^r/2^a$ , where  $a$  is the number of  $d_i$ 's equal to  $m_i/2$ .

The action of  $\text{PO}(U, Q)$  preserves the decomposition of  $U \otimes K$  into generalized eigenspaces, in the sense that

$$U_{i,gTg^{-1}} = gU_{i,T}, \quad \forall T \in V_f(K), \forall g \in \text{PO}(U, Q)(K), \forall i = 1, \dots, r+1.$$

Therefore one obtains a Galois equivariant action of  $\text{PO}(U, Q)$  on  $W_{\{d_1, \dots, d_{r+1}\}}^f$ .

**Theorem 1.39.**  $\text{PO}(U, Q)(K)$  acts on  $W_{\{d_1, \dots, d_{r+1}\}}^f(K)$  simply-transitively if  $a = 0$  and transitively if  $a > 0$ .

**Theorem 1.40.** Suppose  $k$  is arbitrary. Then  $\text{PO}(V, Q)(k')$  acts simply-transitively on  $W_{\{0, \dots, 0\}}^f(k')$  for any field  $k'$  containing  $k$ .

**Proof:** Same descent argument as the proof of Theorem 1.4. □

We begin by studying the conjugation action of  $\text{PO}(U, Q)$  on  $V_f$ .

**Proposition 1.41.** If  $f(x)$  splits completely over  $k$  and  $k = k^2$ , then  $\text{PO}(U, Q)(k)$  acts transitively on  $V_f(k)$ . If  $k$  is arbitrary,  $T \in V_f(k)$  and  $k'$  is any field containing  $k$ , then

$$\text{Stab}_{\text{PO}(U, Q)}(T)(k') = \mu_2(k'[T]^\times)/(\pm 1) \simeq \mu_2(k'[x]/f(x))^\times/(\pm 1).$$

In particular,  $\text{Stab}_{\text{PO}(U, Q)}(T)(K)$  is an elementary abelian 2-group of order  $2^r$ .

**Proof:** The first statement follows in the same way as the proof of Proposition 1.1 except now  $k[x]/f(x)$  is a product of algebras of the form  $k[x]/x^{m_i}$ . Every unit in  $k[x]/x^{m_i}$  is a square if  $k = k^2$  and  $\text{char}(k) \neq 2$ .

The second statement follows from the structure theory of finitely generated modules over Principal Ideal Domains. One can view  $U \otimes k'$  as a module over  $k'[x]$  with  $x$  acting via the operator  $T$ . The elements in  $\text{GL}(U)(k)$  commuting with  $T$  are precisely the automorphisms of  $U$  as a  $k'[x]$ -module. Since  $T$  is regular, the structure theory of finitely generated modules over PID says that  $U \otimes k'$  is isomorphic to  $k'[x]/f(x)$  as a  $k'[x]$ -module. As a module of  $k'[x]$  generated by the element 1, the automorphisms of  $U$  are precisely multiplication by elements in  $(k'[x]/f(x))^\times$ . Then as in Proposition 1.1,

$$\begin{aligned} \text{Stab}_{O(U, Q)}(T)(k') &= \{g(T) \mid g \in k'[x], g(T)^*g(T) = 1\} \\ &= \mu_2(k'[T]^\times) \\ \text{Stab}_{\text{PO}(U, Q)}(T)(k') &= \mu_2(k'[T]^\times)/(\pm 1). \end{aligned}$$

For the last statement, from the factorization of  $f(x)$ , we know

$$K[x]/f(x) \simeq \prod_{i=1}^{r+1} K[x]/(x - \alpha_i)^{m_i}.$$

Therefore,  $\text{Stab}_{O(U, Q)}(T)(K) \simeq (\mathbb{Z}/2\mathbb{Z})^{r+1}$  is an elementary abelian 2-group of order  $2^{r+1}$ . Modding out the diagonally embedded  $\mathbb{Z}/2\mathbb{Z}$  gives  $\text{Stab}_{\text{PO}(U, Q)}(T)(K)$ .  $\square$

**Remark 1.42.** Just as in Remark 1.6, we can give a more explicit description for the stabilizer as polynomials in  $T$ . For each  $i = 1, \dots, r+1$ , define  $h_i^T(x) = f(x)/(x - \alpha_i)^{m_i}$ . Then

$$\begin{aligned}\mu_2(K[T]^\times) &= \left\{ \prod_{i \in I} \left( 1 - 2 \frac{h_i^T(T)}{h_i^T(\alpha_i)} \right) \right\}_{I \subset \{1, \dots, r+1\}} \\ &= \left\{ 1 - 2 \sum_{i \in I} \frac{h_i^T(T)}{h_i^T(\alpha_i)} \right\}_{I \subset \{1, \dots, r+1\}}.\end{aligned}$$

For any  $I \subset \{1, \dots, r+1\}$  and any  $j \notin I$ , since  $(x - \alpha_j)^{m_j}$  divides  $h_i(x)$  in  $K[x]$  and  $(T - \alpha_j)^{m_j}$  kills all the generalized eigenspaces  $U_{j,T}$ ,

$$1 - 2 \sum_{i \in I} \frac{h_i^T(T)}{h_i^T(\alpha_i)}$$

acts trivially on  $U_{j,T}$ .

**Corollary 1.43.** For any  $T, T' \in V_f(K)$ , there exists a bijection

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K) \longleftrightarrow L_{\{d_1, \dots, d_{r+1}\}}^{f,T'}(K).$$

**Proof:** Suppose  $g \in \text{PO}(U, Q)(K)$  conjugates  $T$  to  $T'$ , then the left action by  $g$  on  $\text{Gr}(n, U)$  gives the desired bijection.  $\square$

For any  $T \in V_f(K)$ , its stabilizer  $J_T$  in  $\text{PO}(U, Q)(K)$  acts on  $L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)$ . We rephrase the main theorems as follows.

**Theorem 1.44.** For any  $X \in L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)$ , let  $a$  denote the number of  $d_i$  equal to  $m_i/2$ .

1.  $|\text{Stab}_{J_T}(X)| = 2^a$ .
2.  $|L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)| = 2^r / 2^a$ .

Theorem 1.38 is the second statement and Theorem 1.39 follows because the size of each orbit is

$$|J_T| / |\text{Stab}_{J_T}(X)| = 2^r / 2^a = |L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)|.$$

We will prove Theorem 1.44 via a series of reductions.

**Reduction on  $d_1, \dots, d_{r+1}$**

Suppose  $X \in L_{\{d_1, \dots, d_{r+1}\}}^{f, T}(K)$  with  $d_i \geq 1$ . Let  $v_i$  denote an eigenvector of  $T$  corresponding to  $\alpha_i$ . Since  $T$  is regular,  $v_i$  is unique up to scaling. The assumption  $d_i \geq 1$  then implies  $v_i \in X$ . Let  $H_i$  denote the hyperplane  $v_i^\perp$ , and let  $b$  denote the bilinear form associated to  $Q$ . Note  $v_i \in H_i$  since there exists some  $v'_i$  such that  $(T - \alpha_i)v'_i = v_i$ , and hence

$$b(v_i, v_i) = b(v_i, (T - \alpha_i)v'_i) = b((T - \alpha_i)v_i, v'_i) = 0.$$

For any  $w \in H_i$ ,

$$b(v_i, Tw) = b(Tv_i, w) = b(\alpha_i v_i, w) = 0.$$

Therefore,  $T$  descends to a linear map

$$\overline{T}_i : H_i/v_i \rightarrow H_i/v_i =: \overline{U}_i.$$

The quadratic form  $Q$  descends to a non-degenerate quadratic form  $\overline{Q}_i$  with respect to which  $\overline{T}_i$  is self-adjoint. We claim that  $\overline{T}_i$  is regular with characteristic polynomial  $f(x)/(x - \alpha_i)^2$ . Note this reduction can be described projectively as intersecting the quadric defined by  $Q$  with the tangent plane to  $v_i$ , then projecting away from  $v_i$ .

Indeed, since  $T$  has pairwise orthogonal generalized eigenspaces, the generalized eigenspaces  $U_{j, T}$  corresponding to eigenvalues  $\alpha_j$  not equal to  $\alpha_i$  all lie inside  $H_i$  and map bijectively inside  $\overline{U}_i$  as generalized eigenspaces for  $\overline{T}_i$ . If  $w + \langle v_i \rangle \in \overline{U}_i$  satisfies

$$(\overline{T}_i - \alpha_i)^N(w + \langle v_i \rangle) = \langle v_i \rangle, \quad \text{for some fixed } N$$

then  $(T - \alpha_i)^N w \in \langle v_i \rangle$ . Therefore,

$$\overline{U}_{i, \overline{T}_i} = (U_{i, T} \cap H_i) / v_i$$

is the generalized eigenspace of  $\overline{T}_i$  corresponding to  $\alpha_i$ . Hence its dimension is  $m_i - 2$  and the  $\alpha_i$ -eigenspace of  $\overline{T}_i$  is 1-dimensional.

Since  $v_i \in X$  and  $X$  is isotropic, we see  $X \subset H_i$ . Let  $\overline{X}_i$  denote the image of  $X$  in  $\overline{U}_i$ . It is immediate from the definition that  $\overline{X}_i$  is  $(n - 1)$ -dimensional, satisfying

$$\overline{X}_i \subset \overline{X}_i^{\perp \overline{Q}_i}, \overline{T}_i \overline{X}_i \subset \overline{X}_i^{\perp \overline{Q}_i},$$

and the maximal dimensions of  $\overline{T}_i$ -stable subspaces in its intersection with the generalized eigenspaces are  $d_1, \dots, d_i - 1, \dots, d_{r+1}$ . We denote this reduction step by

$$L_{\{d_1, \dots, d_{r+1}\}}^{f, T}(K) \xrightarrow[\delta]{} L_{\{d_1, \dots, d_i - 1, \dots, d_{r+1}\}}^{f/(x - \alpha_i)^2, \overline{T}_i}(K).$$

$\delta$  is bijective, its inverse is given by taking the pre-image of the projection map  $H_i \rightarrow \overline{U}_i$ .

How are the stabilizers affected by this reduction? If  $h(x)$  is any polynomial in  $K[x]$ , then  $\delta(h(T)X) = h(\overline{T}_i)\overline{X}_i$ . Since  $\delta$  is bijective, we conclude that  $h(T)$  stabilizes  $X$  if and only if  $h(\overline{T}_i)$  stabilizes  $\overline{X}_i$ . Note if  $m_i \geq 3$ , then

$$h_i^T(x) = \frac{f(x)}{(x - \alpha_i)^{m_i}} = \frac{f(x)/(x - \alpha_i)^2}{(x - \alpha_i)^{m_i - 2}} = h_i^{\overline{T}_i}(x).$$

Hence according to the explicit description given in Remark 1.42,

$$h(T) \in J_T \iff h(\overline{T}_i) \in J_{\overline{T}_i}, \quad \text{hence} \quad |\text{Stab}_{J_T}(X)| = |\text{Stab}_{J_{\overline{T}_i}}(\overline{X}_i)|.$$

When  $m_i = 2, d_i = 1$ ,  $\alpha_i$  is no longer an eigenvalue for  $\overline{T}_i$ . In this case,

$$J_T = \langle h(T), 1 - 2h_i(T)/h_i(\alpha_i)|h(\overline{T}_i) \in J_{\overline{T}_i} \rangle.$$

Let  $v'_i$  denote an element in  $U_{i,T}$  such that  $(T - \alpha_i)v'_i = v_i$ . Then

$$U_{i,T} = \text{Span}\{v_i, v'_i\}, \quad \text{and} \quad b(v_i, v'_i) \neq 0.$$

Since  $v_i \in X$  and  $X$  is isotropic, we see

$$X = \text{Span}\{v_i, X \cap \text{Span}\{U_{j,T}\}_{j \neq i}\}.$$

Now  $1 - 2h_i(T)/h_i(\alpha_i)$  sends  $v_i$  to  $-v_i$  and fixes every element in  $\text{Span}\{U_{j,T}\}_{j \neq i}$ . Therefore it stabilizes  $X$  and hence

$$|\text{Stab}_{J_T}(X)| = 2|\text{Stab}_{J_{\overline{T}_i}}(\overline{X}_i)|.$$

Note this case is precisely when  $a$  decreases by 1 in this reduction step.

We summerize this reduction step in the following lemma.

**Lemma 1.45.** Suppose  $d_i \geq 1$ , then there is a bijection

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K) \xrightarrow[\delta]{\sim} L_{\{d_1, \dots, d_i-1, \dots, d_{r+1}\}}^{f/(x-\alpha_i)^2, \overline{T}_i}(K).$$

The sizes of the stabilizers do not change, unless  $m_i = 2, d_i = 1$  in which case it decreases by a factor of 2.

## Reduction on $f$

By the above reduction step, it remains to study  $L_{\{0,0,\dots,0\}}^{f,T}(K)$ . We will describe the reduction map, state the corresponding result, then give the proof. However, since the proof is just hardcore linear algebra, we recommend the interested reader to prove it himself.



Suppose  $\alpha$  is a root of  $f$  of multiplicity  $m \geq 2$ . Let  $X \in L_{\{0,0,\dots,0\}}^{f,T}(K)$  be arbitrary. Let  $v$  denote an eigenvector of  $T$  with eigenvalue  $\alpha$ . Suppose  $v' \in U$  such that  $(T - \alpha)v' = v$ . Since

$$b(v, v) = b(v, (T - \alpha)v') = b((T - \alpha)v, v') = 0,$$

we can consider the descent to  $\overline{U} = v^\perp/v$ . As in the above reduction step,  $Q$  descends to a non-degenerate quadratic form  $\overline{Q}$  on  $\overline{U}$  and  $T$  descends to a regular self-adjoint operator  $\overline{T}$  on  $\overline{U}$  with characteristic polynomial  $f(x)/(x - \alpha)^2$ .

Observe that  $v \notin X$  since  $X$  contains no  $T$ -stable subspace. Therefore the map  $U \rightarrow U/v$  is bijective when restricted to  $X$ . Consequently,  $X \not\subseteq v^\perp$ , for if otherwise the  $(2n - 1)$ -dimensional vector space  $v^\perp/v$  contains an  $n$ -dimensional isotropic subspace which is impossible. Now  $X \cap v^\perp$  has dimension  $n - 1$  and we denote its bijective image in  $v^\perp/v$  by  $\overline{X}$ .

**Lemma 1.46.** The above map sending  $X$  to  $\overline{X}$  defines a surjection

$$L_{\{0,0,\dots,0\}}^{f,T}(K) \longrightarrow L_{\{0,0,\dots,0\}}^{f/(x-\alpha)^2, \overline{T}}(K).$$

This map is bijective if  $m > 2$  and is two-to-one if  $m = 2$ . In both cases,

$$|\text{Stab}_{J_T}(X)| = |\text{Stab}_{J_{\overline{T}}}(\overline{X})|, \quad \text{for any } X \in L_{\{0,\dots,0\}}^{f,T}(K).$$

**Proof:** It is clear that  $\overline{X}$  satisfies  $\overline{X} \subset \overline{X}^\perp, \overline{T}\overline{X} \subset \overline{X}^\perp$ . If  $\overline{X}$  contains a  $\overline{T}$ -stable subspace, then it must contain  $v' + \langle v \rangle$ . Hence  $v' + cv \in X$  for some  $c \in k^s$ . Then  $v = (T - \alpha)(v' + cv) \in X^\perp$  contradicting  $X \not\subseteq v^\perp$ . Therefore,  $\overline{X} \in L_{\{0,0,\dots,0\}}^{f/(x-\alpha)^2, \overline{T}}(k^s)$ . We first prove surjectivity. Suppose  $\overline{X} \in L_{\{0,0,\dots,0\}}^{f/(x-\alpha)^2, \overline{T}}(K)$ . Let  $b_\alpha$  denote the bilinear form

$$b_\alpha(u, u') = b(u, (T - \alpha)u').$$

Since  $v$  lies in the kernel of  $b_\alpha$ , we see that  $b_\alpha$  descends to a non-degenerate bilinear form on the  $2n$  dimensional vector space  $U/v$ . Denote by  $\perp_\alpha$  the perpendicular space with respect to

$b_\alpha$ . Since  $\overline{X}$  is  $n - 1$  dimensional,  $b_\alpha$  further descends to a non-degenerate bilinear form on the 2-dimensional vector space  $\overline{X}^{\perp_\alpha}/\overline{X}$ . It has two 1-dimensional isotropic lines, denote by  $\overline{X}_1, \overline{X}_2$  their pre-images in  $\overline{X}^{\perp_\alpha}$ .

Suppose  $m \geq 3$ , let  $v''$  be an element of  $U$  such that  $(T - \alpha)v'' = v'$ . Then

$$b_\alpha(v', v') = b(v', v) = b((T - \alpha)v'', v) = b(v'', (T - \alpha)v) = 0.$$

Hence we might assume without loss of generality that  $\overline{X}_1 = \text{Span}\{v' + \langle v \rangle, \overline{X}\} \subset v^\perp/v$ . Since  $\text{Span}\{\overline{X}_1, \overline{X}_2\}$  has dimension  $n + 1$ , it is not isotropic with respect to  $b_\alpha$ . Therefore,  $b_\alpha(w, v') = b(w, v) \neq 0$  for some  $w + \langle v \rangle \in \overline{X}_2$ . Up to scaling, we may assume  $b(w, v) = 1$  and by replacing  $w$  by  $w - \frac{1}{2}b(w, w)v$ , we may also assume  $b(w, w) = 0$ . Consider

$$\begin{aligned} X^w &= \text{Span}\{w, u - b(w, u)v\}_{u + \langle v \rangle \in \overline{X}} \subset U, \\ (T - \alpha)X^w &= \text{Span}\{(T - \alpha)w, (T - \alpha)v\}. \end{aligned}$$

It is clear that  $X^w \subset X^{w\perp}$  and  $TX^w \subset X^{w\perp}$  with respect to  $b$  by the construction of  $w$ . Since  $w \notin v^\perp$ , we see  $\overline{X^w} = \overline{X}$ . Since  $b(w, c_2v) = c_2$ ,  $X^w$  contains no non-zero vector of the form  $c_2v$  and hence  $X^w$  contains no non-zero  $T$ -stable subspace. We have now proved surjectivity when  $m \geq 3$ .

Suppose now  $X' \in L_{\{0, \dots, 0\}}^{f, T}(K)$  maps to  $\overline{X}$ . Then the image of  $X'$  in  $U/v$ , denoted suggestively by  $\overline{X'}_2$  is an  $n$ -plane isotropic to  $b_\alpha$ , it contains  $\overline{X}$  and is  $b_\alpha$ -orthogonal to  $\overline{X}$ . Since it does not contain  $v' + \langle v \rangle$ , we conclude that  $\overline{X'}_2 = \overline{X}_2$ . Since the process from  $\overline{X}_2$  to  $X^w$  is just adjusting by adding the correct multiples of  $v$ , we see that  $X' = X^w$ .

Just as in the previous reduction step, when  $m \geq 3$ ,  $J_T$  and  $J_{\overline{T}}$  are represented by the same set of polynomials. It is clear that if  $g(T)$  stabilizes  $X$ , then  $g(\overline{T})$  stabilizes  $\overline{X}$ . Conversely, if  $g(\overline{T})$  stabilizes  $\overline{X}$ , then  $g(T)$  sends  $X$  to another  $n$ -plane that also maps to  $\overline{X}$ . Since there is

only one such  $n$ -plane, we conclude that  $g(T)$  also stabilizes  $X$ . Therefore

$$|\text{Stab}_{J_T}(X)| = |\text{Stab}_{J_{\overline{T}}}(\overline{X})|.$$

We now deal with the case  $m = 2$ . Write  $\overline{X}_1 = \text{Span}\{w_1 + \langle v \rangle, \overline{X}\}$  and  $\overline{X}_2 = \text{Span}\{w_2 + \langle v \rangle, \overline{X}\}$ . We claim  $w_1 \notin v^\perp$  and likewise same with  $w_2$ . If for a contradiction that  $w_1 \in v^\perp$ , then  $\overline{X}_1 \subset v^\perp/v$ . When  $m = 2$ ,  $v^\perp/v$  is the orthogonal (with respect to  $b$ ) direct sum of all the generalized eigenspaces not containing  $v, v'$ . Since  $(T - \alpha)$  acts invertibly on generalized eigenspaces not containing  $v, v'$ , we see that  $b_\alpha$  descends to a non-degenerate bilinear form on  $v^\perp/v$ . However,  $\overline{X}_1$  is isotropic of dimension  $n$  and  $v^\perp/v$  has dimension  $2n - 1$ . Contradiction.

Finally, we lift each  $\overline{X}_i$  to  $X^{w_i}$  by adding an appropriate multiples of  $v$ . The resulting  $X^{w_i}$  both map to  $\overline{X}$  under the reduction map. They are different from each other since their images in  $U/v$  are different. Therefore we have proved surjectivity. The same argument as the above shows that  $X^{w_1}$  and  $X^{w_2}$  are precisely the two pre-images of  $\overline{X}$ .

Regarding stabilizers, we are in the situation where compared to  $J_{\overline{T}}$ ,  $J_T$  has an extra generator  $h_0(T) = 1 - 2h(T)/h(\alpha)$  where  $h(x) = f(x)/(x - \alpha)^2$ . This extra generator fixes  $v$  and acts as  $-1$  on all the other generalized eigenspaces. Therefore  $h_0(\overline{T})\overline{X} = \overline{X}$  and a simple computation shows that it switches  $\overline{X}_1$  and  $\overline{X}_2$ . If  $g(\overline{T})$  stabilizes  $\overline{X}$ , then  $g(T)$  either stabilizes  $X^{w,1}$  or it sends  $X^{w_1}$  to  $X^{w_2}$ , in which case  $g(T)h_0(T)$  stabilizes  $X^{w_1}$ . Therefore, the size of the stabilizers remains unchanged.  $\square$

**Corollary 1.47.**  $|L_{\{0,0,\dots,0\}}^{f,T}(K)| = 2^r$  and every element has trivial stabilizer in  $J_T$ .

**Proof:** This follows from induction on the degree of  $f$  and the classical result on generic intersection in odd dimension recalled in Section 1.1. We write out the proof slightly differently from an induction argument so we can point out the differences between the contributions coming from roots of  $f$  with odd multiplicity and the contributions from roots with even multiplicity.

Rewrite the factorization of  $f(x)$  as

$$f(x) = \prod_{i=1}^{s_1+1} (x - \beta_i)^{2n_i+1} \prod_{j=1}^{s_2} (x - \beta'_j)^{2n'_j},$$

where each  $\beta_i$  is a root of  $f(x)$  of odd multiplicity and each  $\beta'_j$  is a root of even multiplicity. Since  $f(x)$  has odd degree, we know  $s_1 \geq 0$  and  $s_1 + s_2 = r$ . Applying Lemma 1.46 repeatedly, one gets the following sequence of maps,

$$L_{\{0,0,\dots,0\}}^{f,T}(K) \xrightarrow{1 \text{ to } 1} L_{\{0,0,\dots,0\}}^{\prod_i (x-\beta_i) \cdot \prod_j (x-\beta'_j)^2, T'}(K) \xrightarrow{2^{s_2} \text{ to } 1} L_{\{0,0,\dots,0\}}^{\prod_i (x-\beta_i), T''}(K).$$

The last set has  $2^{s_1}$  elements all of whose stabilizers are trivial. Applying Lemma 1.46 again, one concludes that every element in  $L_{\{0,0,\dots,0\}}^{f,T}(K)$  has trivial stabilizer as well. The above diagram shows that  $|L_{\{0,0,\dots,0\}}^{f,T}(K)| = 2^{s_1+s_2} = 2^r$ .  $\square$

**Proof of Theorem 1.44:** Applying Lemma 1.45 repeatedly gives a bijection

$$L_{\{d_1,\dots,d_{r+1}\}}^{f,T}(K) \xrightarrow[\delta]{\sim} L_{\{0,0,\dots,0\}}^{\prod_i (x-\alpha_i)^{m_i-2d_i}, T'}(K),$$

and for any  $X \in L_{\{d_1,\dots,d_{r+1}\}}^{f,T}(K)$ ,

$$|\text{Stab}_{J_T}(X)| = 2^a |\text{Stab}_{J_{T'}}(\delta(X))|.$$

The polynomial  $g(x) = \prod_i (x - \alpha_i)^{m_i-2d_i}$  has  $r+1-a$  distinct roots, hence applying Corollary 1.47 to  $g$  completes the proof.  $\square$

## 1.5 Even dimension, regular case

In this section, we generalize Section 1.2 to the case where the self-adjoint operator  $T$  is **regular**. The idea is to reduce from the regular case to the generic case using a series of reductions similar to the ones used in Section 1.4. We start with the study of a simply-transitive action of PSO as

the reduction steps are simpler.

### 1.5.1 Torsor for $J[2]$

Suppose  $U$  is a  $k$ -vector space of dimension  $2n + 2$  and let  $Q$  be a quadratic form on  $U$  of discriminant 1. Fix a ruling  $Y_0$  of  $(n + 1)$ -dimensional isotropic subspace of  $Q$ . Note  $Y_0$  is defined over  $k$  because the rulings are defined over  $k(\sqrt{\text{disc}(Q)})$ .

Let  $f$  be a monic polynomial of degree  $2n + 2$  splitting completely over  $k^s$  and let  $J$  denote the Jacobian of the hyperelliptic curve  $C$  defined by  $y^2 = f(x)$ . We define the  $k$ -scheme,

$$V_f = \{T : U \rightarrow U \mid T \text{ is self-adjoint and regular with characteristic polynomial } f(x)\}.$$

Note here regularity means there is no linear relations between  $1, T, \dots, T^{2n+1}$ . For every field  $k'$  containing  $k$ , and every  $T \in V_f(k')$ , let  $W_T(k')$  denote the set of (linear)  $n$ -dimensional  $k'$ -subspaces  $X$  of  $U \otimes k'$  such that  $\text{Span}\{X, TX\} \sim Y_0$ . That is to say the linear space  $\text{Span}\{X, TX\}$  is an  $(n + 1)$ -dimensional isotropic subspace with respect to  $Q$  that lies inside the ruling  $Y_0$  over  $k'$ . As before, we define

$$W_f(k') = \{(T, X) \mid T \in V_f(k'), X \in W_T(k')\}.$$

There is a Galois invariant action of  $\text{PSO}(U, Q) = \text{SO}(U, Q)/(\pm 1)$  on  $W_f$  :

$$g.(T, X) = (gTg^{-1}, gX).$$

Let  $K$  be either the separable closure or algebraic closure of  $k$ , and suppose  $f(x)$  factors as  $f(x) = \prod_{i=1}^{r+1} (x - \alpha_i)^{m_i}$  for  $\alpha_i \in K$ . In fact, we only need  $K$  to be a field over which  $f$  splits completely and that  $K = K^2$ ; but since we will not use the result in any case other than  $K = k^s, k^s$ , we will assume for the convenience of the reader that  $K$  is  $k^s$  or  $k^s$ . For any  $T \in V_f(K)$ , one can decompose  $U \otimes K$  into generalized  $T$ -eigenspaces. Namely,  $U \otimes K = \bigoplus_{i=1}^{r+1} U_{i,T}$  where

each  $U_{i,T} \subset_K U$  is an  $m_i$ -dimensional  $K$ -subspace of  $U \otimes K$ . For any self-adjoint  $T$ , its generalized eigenspaces are pairwise orthogonal with respect to  $Q$ . Therefore  $Q$  restricts to non-degenerate quadratic forms on each  $U_{i,T}$ . For any  $X \in W_T(K)$ ,  $\text{Span}\{X, TX\} \cap U_{i,T}$  is isotropic and therefore has dimension at most  $m_i/2$ . For any sequence of integers  $d_1, \dots, d_{r+1}$  such that  $0 \leq d_i \leq m_i/2$ , for any intermediate field  $k'$  between  $k$  and  $K$ , and for any  $T \in V_f(k')$ , we define

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(k') = \{X \in W_T(k') \mid \dim(\text{maximal } T\text{-stable subspace of } (\text{Span}_K\{X, TX\}) \cap U_{i,T}) = d_i\},$$

$$W_{\{d_1, \dots, d_{r+1}\}}^f(k') = \{(T, X) \mid T \in V_f(k'), X \in L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(k')\}.$$

Note when  $f$  has no repeated roots, all  $m_i$  equal to 1, all  $d_i$  are 0 and  $L_{\{0, \dots, 0\}}^{f,T}(k')$ ,  $W_{\{0, \dots, 0\}}^f(k')$  recover  $W_T(k')$ ,  $W_f(k')$  respectively. Note it is important that the integers  $d_i$  are defined as the dimension of  $T$ -stable subspaces inside  $\text{Span}\{X, TX\} \cap U_{i,T}$ , not just  $X \cap U_{i,T}$  as we did in the odd case. If we used the latter definition, then  $L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)$  will be infinite whenever  $f(x)$  has a root of multiplicity at least 4. See Example 1.62 and Example 1.63.

In what follows, we impose the following condition

$$d_1 + \dots + d_{r+1} < n + 1 = \dim \text{Span}\{X, TX\}. \quad (1.11)$$

This condition is equivalent to saying  $\text{Span}\{X, TX\}$  is not  $T$ -stable. Let  $s_1$  denote the number of roots of  $f$  with odd multiplicity. Then the maximum  $d_1 + \dots + d_{r+1}$  could reach is  $n + 1 - s_1/2$ . If (1.11) fails, then we must have  $s_1 = 0$  and hence  $C$  is reducible. If one uses  $L^{f,T}$  instead of  $L'^{f,T}$  or if one does not assume (1.11), then there will be infinitely many choices for  $X$  when  $C$  is reducible. See Example 1.62 and Example 1.63.

As one would expect from the odd case, the main theorem we are heading towards is the following:

**Theorem 1.48.** Suppose  $d_1 + \dots + d_{r+1} < n + 1$ , then  $|L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)| = 2^r/2^a$ , where  $a$  is the number of  $d_i$ 's equal to  $m_i/2$ .

The action of  $\text{PSO}(U, Q)$  preserves the decomposition of  $U \otimes K$  into generalized eigenspaces. Therefore one obtains a Galois invariant action of  $\text{PSO}(U, Q)$  on  $W_{\{d_1, \dots, d_{r+1}\}}^f$ .

**Theorem 1.49.** Suppose  $d_1 + \dots + d_{r+1} < n + 1$ , then  $\text{PSO}(U, Q)(K)$  acts on  $W_{\{d_1, \dots, d_{r+1}\}}^f(K)$  simply-transitively if  $a = 0$  and transitively if  $a > 0$ .

**Theorem 1.50.** Suppose  $k$  is arbitrary and  $d_1 + \dots + d_{r+1} < n + 1$ . Then  $\text{PSO}(V, Q)(k')$  acts simply-transitively on  $W_{\{0, \dots, 0\}}^f(k')$  for any field  $k'$  containing  $k$ .

**Proof:** Same descent argument as the proof of Theorem 1.4. □

We begin by studying the conjugation action of  $\text{PSO}(U, Q)$  on  $V_f$ .

**Proposition 1.51.** If  $f(x)$  splits completely over  $k$  and  $k = k^2$ , then  $\text{PO}(U, Q)(k)$  acts transitively on  $V_f(k)$ . If  $k$  is arbitrary,  $T \in V_f(k)$  and  $k'$  is any field containing  $k$ , then

$$\text{Stab}_{\text{PSO}(U, Q)}(T)(k') = (\mu_2(k'[T]^\times)/(\pm 1))_{N=1} \simeq (\mu_2(k'[x]/f(x))^\times/(\pm 1))_{N=1} \simeq J[2](k').$$

In particular,  $\text{Stab}_{\text{PSO}(U, Q)}(T)(K)$  is an elementary abelian 2-group of order  $2^r$ .

**Proof:** cf. Proposition 1.41. □

**Remark 1.52.** A more explicit description for the stabilizer as polynomials in  $T$  is almost identical to the odd case as given in Remark 1.42. For each  $i = 1, \dots, r + 1$ , define  $h_i^T(x) = f(x)/(x - \alpha_i)^{m_i}$ . Then

$$\begin{aligned} \mu_2(K[T]^\times) &= \left\{ \prod_{i \in I} \left( 1 - 2 \frac{h_i^T(T)}{h_i^T(\alpha_i)} \right) \right\}_{I \subset \{1, \dots, r+1\}, 2 \mid |I|} \\ &= \left\{ 1 - 2 \sum_{i \in I} \frac{h_i^T(T)}{h_i^T(\alpha_i)} \right\}_{I \subset \{1, \dots, r+1\}, 2 \mid |I|}. \end{aligned}$$

For any  $I \subset \{1, \dots, r + 1\}$  and any  $j \notin I$ , since  $(x - \alpha_j)^{m_j}$  divides  $h_i(x)$  in  $K[x]$  and  $(T - \alpha_j)^{m_j}$

kills all the generalized eigenspaces  $U_{j,T}$ ,

$$1 - 2 \sum_{i \in I} \frac{h_i^T(T)}{h_i^T(\alpha_i)}$$

acts trivially on  $U_{j,T}$ .

**Corollary 1.53.** For any  $T, T' \in V_f(K)$ , there exists a bijection

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K) \longleftrightarrow L_{\{d_1, \dots, d_{r+1}\}}^{f,T'}(K).$$

**Proof:** Suppose  $g \in \text{PO}(U, Q)(K)$  conjugates  $T$  to  $T'$ , then the left action by  $g$  on  $\text{Gr}(n, U)$  gives the desired bijection.  $\square$

Also by Proposition 1.41, for any  $T \in V_f(K)$ , its stabilizer  $J_T$  in  $\text{PSO}(U, Q)(K)$  acts on  $L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)$ . We rephrase the main theorems as follows.

**Theorem 1.54.** Suppose  $d_1 + \dots + d_{r+1} < n + 1$ . For any  $X \in L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)$ , let  $a$  denote the number of  $d_i$  equal to  $m_i/2$ .

1.  $|\text{Stab}_{J_T}(X)| = 2^a$ .
2.  $|L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)| = 2^r / 2^a$ .

Theorem 1.48 is the second statement and Theorem 1.49 follows because the size of each orbit is

$$|J_T| / |\text{Stab}_{J_T}(X)| = 2^r / 2^a = |L_{\{d_1, \dots, d_{r+1}\}}^{f,T}(K)|.$$

We will prove Theorem 1.44 via a series of reductions.

One major difference from the odd case is that one should forget about the rulings in the following reductions. Namely, consider instead

$$W_T^*(K) = \{X \in \text{Gr}(n, U \otimes K) \mid \text{Span}\{X, TX\} \text{ is } n+1 \text{ dimensional and isotropic}\}.$$



Observe that  $W_T^*(K)$  has two components, one of which is  $W_T(K)$ , corresponding to which ruling  $\text{Span}\{X, TX\}$  lies in. The two components are in bijection to each other via an element in  $\text{Stab}_{PO}(T)$  but not in  $\text{Stab}_{PSO}(T)$ . One defines similarly  $L_{\{d_1, \dots, d_{r+1}\}}^{f, T, *}(K)$ .

### Reduction on $d_1, \dots, d_{r+1}$

Suppose  $X \in L_{\{d_1, \dots, d_{r+1}\}}^{f, T, *}(K)$  with  $d_i \geq 1$ . Let  $v_i$  denote an eigenvector of  $T$  corresponding to  $\alpha_i$ . Since  $T$  is regular,  $v_i$  is unique up to scaling. The assumption  $d_i \geq 1$  implies  $v_i \in \text{Span}\{X, TX\}$ . Hence

$$X \subset \text{Span}\{X, TX\}^\perp \subset v_i^\perp =: H_i.$$

Let  $b$  denote the bilinear form associated to  $Q$ . For any  $w \in H_i$ ,

$$b(v_i, Tw) = b(Tv_i, w) = b(\alpha_i v_i, w) = 0.$$

Therefore,  $T$  descends to a linear map

$$\overline{T}_i : H_i/v_i \rightarrow H_i/v_i =: \overline{U}_i.$$

The quadratic form  $Q$  descends to a non-degenerate quadratic form  $\overline{Q}_i$  with respect to which  $\overline{T}_i$  is self-adjoint. Just as in the odd case,  $\overline{T}_i$  is regular with characteristic polynomial  $f(x)/(x - \alpha_i)^2$ . Let  $\overline{X}_i$  denote the image of  $X$  in  $\overline{U}_i$ . Then  $\text{Span}\{\overline{X}_i, \overline{T}_i \overline{X}_i\}$  is an isotropic  $n$ -plane with respect to  $\overline{Q}_i$ , and the maximal dimensions of  $\overline{T}_i$ -stable subspaces in the intersection of  $\text{Span}\{\overline{X}_i, \overline{T}_i \overline{X}_i\}$  with the generalized eigenspaces are  $d_1, \dots, d_i - 1, \dots, d_{r+1}$ . Condition (1.11) then tells us  $\overline{X}_i$  is not  $\overline{T}_i$ -stable. Therefore  $v_i \in X$  and  $\overline{X}_i$  is  $n - 1$  dimensional. We denote this reduction step by

$$L_{\{d_1, \dots, d_{r+1}\}}^{f, T, *}(K) \xrightarrow[\delta]{} L_{\{d_1, \dots, d_i - 1, \dots, d_{r+1}\}}^{f/(x - \alpha_i)^2, \overline{T}_i, *}(K).$$

$\delta$  is bijective, its inverse is given by taking the pre-image of the projection map  $H_i \rightarrow \overline{U}_i$ .

The stabilizers are affected in the same manner as in the odd case. We summerize this

reduction step in the following lemma.

**Lemma 1.55.** Suppose  $d_i \geq 1$ , then there is a bijection

$$L_{\{d_1, \dots, d_{r+1}\}}^{f, T, *} (K) \xrightarrow[\delta]{\sim} L_{\{d_1, \dots, d_i-1, \dots, d_{r+1}\}}^{f/(x-\alpha_i)^2, \bar{T}_i, *} (K).$$

The sizes of the stabilizers do not change, unless  $m_i = 2, d_i = 1$  in which case it decreases by a factor of 2.

This reduction can be described projectively as intersecting the quadric defined by  $Q$  with the tangent plane to  $v$ , then projecting away from  $v$ . Such an operation does not preserve the rulings. Two (projective)  $n$ -planes in  $Q$  lying in the same ruling could be sent to different rulings via this procedure. For example take a smooth quadric in  $\mathbb{P}^7$ , and two 3-planes  $Y_1, Y_2$  on the quadric intersecting at a line. Then these two 3-planes lie on the same ruling. If the tangent plane to  $v$  contains this line, then the images of  $Y_1, Y_2$  lie in different rulings since their intersection codimension is 1. If the tangent plane to  $v$  meets this line at a point, then the images  $Y_1, Y_2$  lie in the same ruling as their intersection codimension is 2. Similar examples can be written down when  $Y_1, Y_2$  lie on different rulings.

### Reduction on $f$

By the above reduction step, it remains to study  $L_{\{0,0,\dots,0\}}^{f, T, *} (K)$ . We will describe the reduction map, state the corresponding result, then give the proof. There is a slight difference to the odd case due to dimension reasons. Once again, the proof is just hardcore linear algebra, so we recommend the interested reader to prove it himself.

Suppose  $\alpha$  is a root of  $f$  of multiplicity  $m \geq 2$ . Let  $X \in L_{\{0,0,\dots,0\}}^{f, T, *} (K)$  be arbitrary. Let  $v$  denote an eigenvector of  $T$  with eigenvalue  $\alpha$ . Suppose  $v' \in U$  such that  $(T - \alpha)v' = v$ . Since  $b(v, v) = 0$ , we can consider the descent to  $\bar{U} = v^\perp/v$ . As in the above reduction step,  $Q$  descends to a non-degenerate quadratic form  $\bar{Q}$  on  $\bar{U}$  and  $T$  descends to a regular self-adjoint operator  $\bar{T}$  on  $\bar{U}$  with characteristic polynomial  $f(x)/(x - \alpha)^2$ .

Observe that  $v \notin \text{Span}\{X, TX\}$  since  $\text{Span}\{X, TX\}$  contains no non-zero  $T$ -stable subspace. Therefore the map  $U \rightarrow U/v$  is bijective when restricted to  $\text{Span}\{X, TX\}$ . Denote the image of  $X \cap v^\perp$  in  $\bar{U} = v^\perp/v$  by  $\bar{X}$ . As in the above reduction step,  $\text{Span}\{\bar{X}, \bar{TX}\}$  is an  $n$ -dimensional isotropic subspace of  $\bar{U}$ .

**Lemma 1.56.**  $\text{Span}\{\bar{X}, \bar{TX}\}$  has no non-zero  $\bar{T}$ -stable subspace.

**Proof:** Its only possible non-zero  $\bar{T}$ -stable subspace is the line spanned by  $v' + \langle v \rangle$ . Suppose for a contradiction that  $v' + cv \in \text{Span}\{X, TX\}$  for some  $c \in k$ . Since  $\text{Span}\{X, TX\}$  has no non-zero  $T$ -stable subspace, we see that  $v', v' + cv \notin X$ . Since  $\text{Span}\{X, TX\}$  is isotropic, we see that  $v' + cv$  is orthogonal to every element in  $(T - \alpha)X$ , and hence  $v$  is orthogonal to every element of  $X$ . Since  $v' + cv$  also lies in  $X^\perp$ , we see that  $v' \in X^\perp$ . Finally,  $b(v, v') = 0$  a priori due to the assumption that  $v' + \langle v \rangle \in \bar{U}$ . Combining these, one concludes that the  $(n+2)$ -dimensional subspace  $\text{Span}\{X, v', v\}$  is isotropic in  $U$  with respect to  $b$ , contradicting to the fact that  $U$  only has dimension  $2n+2$ .  $\square$

Consequently,  $X \not\subseteq v^\perp$ , for if otherwise  $\bar{X} = \text{Span}\{\bar{X}, \bar{TX}\}$  for dimension reasons and hence is  $\bar{T}$ -stable, which contradicts both Lemma 1.70 and Condition 1.11. One now has the following well-defined map.

**Lemma 1.57.** Suppose  $n \geq 2$ . The map sending  $X$  to  $\bar{X}$  defines a surjection

$$L_{\{0,0,\dots,0\}}^{f,T,*}(K) \longrightarrow L_{\{0,0,\dots,0\}}^{f/(x-\alpha)^2,\bar{T},*}(K).$$

This map is bijective if  $m > 2$  and is two-to-one if  $m = 2$ . In both cases,

$$|\text{Stab}_{J_T}(X)| = |\text{Stab}_{J_{\bar{T}}}(\bar{X})|, \quad \text{for any } X \in L_{\{0,\dots,0\}}^{f,T}(K).$$

**Proof:** We first prove surjectivity. Suppose  $\bar{X} \in L_{\{0,0,\dots,0\}}^{f/(x-\alpha)^2,\bar{T},*}(K)$ . Let  $b_\alpha$  denote the bilinear form

$$b_\alpha(u, u') = b(u, (T - \alpha)u').$$

Since  $v$  lies in the kernel of  $b_\alpha$ , we see that  $b_\alpha$  descends to a non-degenerate bilinear form on the  $2n+1$  dimensional vector space  $U/v$ . Denote by  $\perp_\alpha$  the perpendicular space with respect to  $b_\alpha$ . Suppose for a contradiction that  $\text{Span}\{\overline{X}, \overline{TX}\}$  is isotropic with respect to  $b_\alpha$ . Then inside  $\overline{U}$ ,

$$\overline{T^2X} \subset \text{Span}\{\overline{X}, \overline{TX}\}^\perp = \text{Span}\{\overline{X}, \overline{TX}\}.$$

Hence the entire  $\text{Span}\{\overline{X}, \overline{TX}\}$  is  $\overline{T}$ -stable. Contradiction.

Observe that  $b_\alpha$  descends to a non-degenerate bilinear form on the 2-dimensional vector space  $\overline{Y} = \text{Span}\{\overline{X}, \overline{TX}\}^{\perp_\alpha} / \overline{X}$ . Indeed a priori,  $b_\alpha$  descends to a non-degenerate form on  $\overline{X}^{\perp_\alpha} / \overline{X}$ , and  $\overline{X}^{\perp_\alpha}$  is spanned by  $\text{Span}\{\overline{X}, \overline{TX}\}^{\perp_\alpha}$  and a non-isotropic vector  $u$  in  $\overline{TX}$ . Given any  $w \in \text{Span}\{\overline{X}, \overline{TX}\}^{\perp_\alpha}$ , one can first find a  $w' \in \overline{X}^{\perp_\alpha}$  such that  $b_\alpha(w, w') \neq 0$ , then adjust  $w'$  by a multiple of  $u$  so it lands in  $\text{Span}\{\overline{X}, \overline{TX}\}$ .

As a 2-dimensional non-degenerate quadratic space,  $\overline{Y}$  has two 1-dimensional isotropic lines, denote by  $\overline{X}_1, \overline{X}_2$  their pre-images in  $\text{Span}\{\overline{X}, \overline{TX}\}^{\perp_\alpha}$ .

Suppose  $m \geq 3$ , then as in the odd case,  $b_\alpha(v', v') = b(v', v) = 0$ , so up to renaming,  $\overline{X}_1 = \text{Span}\{v' + \langle v \rangle, \overline{X}\} \subset v^\perp / v$ . Since  $\text{Span}\{\overline{X}_1, \overline{X}_2\}$  has dimension  $n+1$ , it is not isotropic with respect to  $b_\alpha$ . Therefore,  $b_\alpha(w, v') = b(w, v) \neq 0$  for some  $w + \langle v \rangle \in \overline{X}_2$ . Up to scaling, we may assume  $b(w, v) = 1$  and by replacing  $w$  by  $w - \frac{1}{2}b(w, w)v$ , we may also assume  $b(w, w) = 0$ . Consider

$$\begin{aligned} X^w &= \text{Span}\{w, u - b(w, u)v\}_{u + \langle v \rangle \in \overline{X}} \subset U, \\ (T - \alpha)X^w &= \text{Span}\{(T - \alpha)w, (T - \alpha)v\}. \end{aligned}$$

It is clear that  $\text{Span}\{X^w, TX^w\}$  is isotropic with respect to  $b$  by the construction of  $w$ . Since  $w \notin v^\perp$ , we have  $\overline{X^w} = \overline{X}$ . Since  $b(w, c_2v) = c_2$ , we see that  $\text{Span}\{X^w, TX^w\}$  contains no elements of the form  $c_2v$  since it is isotropic. Therefore  $\text{Span}\{X^w, TX^w\}$  has no non-zero  $T$ -stable subspace. We have now proved surjectivity when  $m \geq 3$ .

Suppose now  $X' \in L_{\{0, \dots, 0\}}^{f, T, *}(K)$  maps to  $\overline{X}$ . Then the image of  $X'$  in  $U/v$ , denoted suggestively

by  $\overline{X}'_2$  is an  $n$ -plane isotropic to  $b_\alpha$ , it contains  $\overline{X}$  and is  $b_\alpha$ -orthogonal to  $\text{Span}\{\overline{X}, \overline{TX}\}$ . Since it does not contain  $v' + \langle v \rangle$ , we conclude that  $\overline{X}'_2 = \overline{X}_2$ . Since the process from  $\overline{X}_2$  to  $X^w$  is just adjusting with the correct multiples of  $v$ , we see that  $X' = X^w$ . The way how the stabilizer changes is identical to the odd case.

We now deal with the case  $m = 2$ . Write  $\overline{X}_1 = \text{Span}\{w_1 + \langle v \rangle, \overline{X}\}$  and  $\overline{X}_2 = \text{Span}\{w_2 + \langle v \rangle, \overline{X}\}$ . We claim  $w_1 \notin v^\perp$  and likewise same with  $w_2$ . Suppose for a contradiction that  $w_1 \in v^\perp$ . Since  $\text{Span}\{\overline{X}, \overline{TX}\}$  is not isotropic with respect to  $b_\alpha$ , we see that  $\text{Span}\{\overline{X}, \overline{TX}, w_1 + \langle v \rangle\}$  is an  $n+1$  dimensional subspace of  $v^\perp/v$ . As in the odd case,  $b_\alpha$  is non-degenerate on  $v^\perp/v$  because  $T - \alpha$  acts invertibly on  $v^\perp/v$ . However, taking  $\perp_\alpha$  inside  $v^\perp/v$ , we see that

$$\text{Span}\{\overline{X}, \overline{TX}, w_1 + \langle v \rangle\}^{\perp_\alpha} \supset \overline{X}_1.$$

The left hand side has dimension  $n-1$  while the right hand side has dimension  $n$ . Contradiction.

Finally, we lift each  $\overline{X}_i$  to  $X^{w_i}$  by adding an appropriate multiples of  $v$ . The resulting  $X^{w_i}$  both maps to  $\overline{X}$  under the reduction map. They are different from each other since their images in  $U/v$  are different. Therefore we have proved surjectivity. The same argument as the above shows that  $X^{w_1}$  and  $X^{w_2}$  are precisely the two pre-images of  $\overline{X}$ . Stabilizers behave in the same way as the odd case.  $\square$

**Corollary 1.58.**  $|L_{\{0,0,\dots,0\}}^{f,T,*}(K)| = 2^{r+1}$  and every element has trivial stabilizer in  $J_T$ .

**Proof:** Apply the reduction steps like in the odd case. There are now five base cases which we illustrate as examples.  $\square$

**Example 1.59.** (Generic case) Suppose reduction terminates with  $f(x) = \prod_{i=1}^{r+1} (x - \alpha_i)$  with  $r \geq 3$ . In this case, one can apply the theory for the nonsingular case discussed in Section 1.2.2 and get  $|L^{f,T,*}| = 2|L^{f,T}| = 2^{r+1}$ .

**Example 1.60.** Suppose reduction terminates with  $f(x) = (x - \alpha)(x - \beta)(x - \gamma)^2$ . If one tries to apply reduction again on  $\gamma$ , then  $\overline{X}$  becomes 0-dimensional. Let  $u, v, w_1$  denote the eigenvectors

of  $T$  with eigenvalue  $\alpha, \beta, \gamma$  respectively and let  $w_2$  be such that  $(T - \gamma)w_2 = w_1$ . We seek coefficients  $c_1, \dots, c_4$  such that  $X = \langle c_1u + c_2v + c_3w_1 + c_4w_2 \rangle$  lies in  $L_{0,0,0}^{f,T,*}(K)$ . Set

$$\Omega_1 = b(u, u) \neq 0, \quad \Omega_2 = b(v, v) \neq 0, \quad \Gamma_3 = b(w_1, w_2) \neq 0, \quad \Gamma_4 = b(w_2, w_2).$$

Then the condition that  $\text{Span}\{X, TX\}$  is an isotropic 2-plane becomes:

$$\begin{pmatrix} \Omega_1 & \Omega_2 & \Gamma_3 & \Gamma_4 \\ (\gamma - \alpha)\Omega_1 & (\gamma - \beta)\Omega_2 & 0 & \Gamma_3 \\ (\gamma - \alpha)^2\Omega_1 & (\gamma - \beta)^2\Omega_2 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_1^2 \\ c_2^2 \\ 2c_3c_4 \\ c_4^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Since  $\Gamma_3, \Omega_1, \Omega_2$  are nonzero, the above matrix has a 1-dimensional kernel. Moreover, if any one of  $c_1, c_2, c_4$  is zero, then they are all zero and  $X$  is of the form  $\langle c_3w_1 \rangle$  which does not lie in  $L_{0,0,0}^{f,T,*}(K)$ . Now, given non-zero  $c_1, c_2, c_4$ , one gets a unique solution for  $c_3$ . Therefore, there are  $8 = 2^3$  choices for  $X$  depending on which square roots one chooses for  $c_1, c_2, c_4$ .

**Example 1.61.** Suppose reduction terminates with  $f(x) = (x - \alpha)^3(x - \beta)$ . Let  $u_1, v$  denote the eigenvectors of  $T$  with eigenvalue  $\alpha, \beta$  respectively and let  $u_2, u_3$  be such that  $(T - \alpha)^2u_3 = (T - \alpha)u_2 = u_1$ . We seek coefficients  $c_1, \dots, c_4$  such that  $X = \langle c_1u_1 + c_2u_2 + c_3u_3 + c_4v \rangle$  lies in  $L_{0,0}^{f,T,*}(K)$ . Set

$$\Omega = b(v, v) \neq 0, \quad \Gamma_4 = b(u_1, u_3) = b(u_2, u_2) \neq 0, \quad \Gamma_5 = b(u_2, u_3), \quad \Gamma_6 = b(u_3, u_3).$$

Then the condition that  $\text{Span}\{X, TX\}$  is an isotropic 2-plane becomes:

$$\begin{pmatrix} \Gamma_4 & \Gamma_5 & \Gamma_6 & \Omega \\ 0 & \Gamma_4 & \Gamma_5 & (\beta - \alpha)\Omega \\ 0 & 0 & \Gamma_4 & (\beta - \alpha)^2\Omega \end{pmatrix} \begin{pmatrix} c_2^2 + 2c_1c_3 \\ 2c_2c_3 \\ c_3^2 \\ c_4^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Since  $\Gamma_4, \Omega$  are nonzero, the above matrix has a 1-dimensional kernel and if any one of  $c_2, c_3, c_4$  is zero, then all of them are zero and  $X$  is of the form  $\langle c_1 u_1 \rangle$  which does not lie in  $L_{0,0}^{f,T,*}(K)$ . Now, given non-zero  $c_3, c_4$ , one gets a unique solution for  $c_1, c_2$ . Therefore, there are  $4 = 2^2$  choices for  $X$  depending on which square roots one chooses for  $c_3, c_4$ .

**Example 1.62.** Suppose reduction terminates with  $f(x) = (x - \alpha)^2(x - \beta)^2$ . Let  $u_1, v_1$  denote the eigenvectors of  $T$  with eigenvalue  $\alpha, \beta$  respectively and let  $u_2, v_2$  be such that  $(T - \alpha)u_2 = u_1, (T - \beta)v_2 = v_1$ . We seek coefficients  $c_1, \dots, c_4$  such that  $X = \langle c_1 u_1 + c_2 u_2 + c_3 v_1 + c_4 v_2 \rangle$  lies in  $L_{0,0}^{f,T,*}(K)$ . Set

$$\Gamma_3 = b(u_1, u_2) \neq 0, \quad \Gamma_4 = b(u_2, u_2), \quad \Omega_3 = b(v_1, v_2) \neq 0, \quad \Omega_4 = b(v_2, v_2).$$

Then the condition that  $\text{Span}\{X, TX\}$  is an isotropic 2-plane becomes:

$$\begin{pmatrix} \Gamma_3 & \Gamma_4 & \Omega_3 & \Omega_4 \\ 0 & \Gamma_3 & (\beta - \alpha)\Omega_3 & \Omega_3 + (\beta - \alpha)\Omega_4 \\ 0 & 0 & (\beta - \alpha)^2\Omega_3 & 2(\beta - \alpha)\Omega_3 + (\beta - \alpha)^2\Omega_4 \end{pmatrix} \begin{pmatrix} 2c_1c_2 \\ c_2^2 \\ 2c_3c_4 \\ c_4^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Since  $\Gamma_3, \Omega_3$  are nonzero, the above matrix has a 1-dimensional kernel. If any one of  $c_2, c_4$  is zero, then both of them are zero and  $X$  is of the form  $\langle c_1 u_1 + c_3 v_1 \rangle$ . In this case,  $\text{Span}\{X, TX\}$  either contains  $\langle u_1 \rangle$  or  $\langle v_1 \rangle$  both of which are  $T$ -stable thereby forcing  $X \notin L_{0,0}^{f,T,*}(K)$ . Note if  $c_1$  and  $c_3$  are both non-zero, then  $X$  satisfy the weaker condition that  $X$  contains no non-zero  $T$ -stable subspace. Moreover,  $X \in L_{1,1}^{f,T,*}(K)$  violates Condition (1.11). It is clear that there are infinitely many such  $X$ .

Now, given non-zero  $c_2, c_4$ , one gets a unique solution for  $c_1, c_3$ . Therefore, there are  $4 = 2^2$  choices for  $X$  depending on which square roots one chooses for  $c_2, c_4$ .

**Example 1.63.** Suppose reduction terminates with  $f(x) = (x - \alpha)^4$ . Let  $u_1$  denote the eigenvector

of  $T$  with eigenvalue  $\alpha$  and let  $u_2, u_3, u_4$  be such that

$$(T - \alpha)^3 u_4 = (T - \alpha)^2 u_3 = (T - \alpha) u_2 = u_1.$$

We seek coefficients  $c_1, \dots, c_4$  such that  $X = \langle c_1 u_1 + c_2 u_2 + c_3 u_3 + c_4 u_4 \rangle$  lies in  $L_0^{f,T,*}(K)$ . Set

$$\Gamma_5 = b(u_1, u_4) \neq 0, \quad \Gamma_6 = b(u_2, u_4) = b(u_3, u_3), \quad \Gamma_7 = b(u_3, u_4), \quad \Gamma_8 = b(u_4, u_4).$$

Then the condition that  $\text{Span}\{X, TX\}$  is an isotropic 2-plane becomes:

$$\begin{pmatrix} \Gamma_5 & \Gamma_6 & \Gamma_7 & \Gamma_8 \\ 0 & \Gamma_5 & \Gamma_6 & \Gamma_7 \\ 0 & 0 & \Gamma_5 & \Gamma_6 \end{pmatrix} \begin{pmatrix} 2c_1 c_4 + 2c_2 c_3 \\ 2c_2 c_4 + c_3^2 \\ 2c_3 c_4 \\ c_4^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Since  $\Gamma_5$  is nonzero, the above matrix has a 1-dimensional kernel and if  $c_4$  is zero, then  $c_3$  is also zero. In this case, any  $X$  of the form  $\langle c_1 u_1 + c_2 u_2 \rangle$  solves the above equation. However, for all such lines,  $\text{Span}\{X, TX\}$  contains the  $T$ -stable subspace  $\langle u_1 \rangle$  thereby forcing  $X \notin L_0^{f,T,*}(K)$ . Note if  $c_1 \neq 0$ , then  $\text{Span}\{X, TX\} = \langle u_1, u_2 \rangle$  and  $X \in L_2^{f,T,*}(K)$  violating Condition 1.11 while all such  $X$  still satisfy the weaker condition that it contains no non-zero  $T$ -stable subspace.

Now, given a non-zero  $c_4$ , one gets a unique solution for  $c_1, c_2, c_3$ . Therefore, there are  $2 = 2^1$  choices for  $X$  depending on which square root one chooses for  $c_4$ .

**Proof of Theorem 1.54:** Applying Lemma 1.55 repeatedly gives a bijection

$$L_{\{d_1, \dots, d_{r+1}\}}^{f,T,*}(K) \xrightarrow[\delta]{\sim} L_{\{0,0,\dots,0\}}^{\prod_i (x-\alpha_i)^{m_i-2d_i}, T',*}(K),$$

and for any  $X \in L_{\{d_1, \dots, d_{r+1}\}}^{f,T,*}(K)$ ,

$$|\text{Stab}_{J_T}(X)| = 2^a |\text{Stab}_{J_{T'}}(\delta(X))|.$$



The polynomial  $g(x) = \prod_i (x - \alpha_i)^{m_i - 2d_i}$  has  $r + 1 - a$  distinct roots, hence applying Corollary 1.58 to  $g$  then dividing by 2 to go from  $|L^{f,T,*}|$  to  $|L^{f,T}|$  completes the proof.  $\square$

### 1.5.2 Torsor for $J$

Suppose now  $U$  has dimension  $N = 2n + 2$  for  $n \geq 1$ . As above, suppose  $Q = Q_1$  is non-degenerate and denote by  $T$  the associated self-adjoint operator on  $U$ . As in Section 1.2.1, let  $C$  be the (possibly singular) hyperelliptic curve parameterizing the rulings in the pencil. It is isomorphic over  $k$ , not canonically, to the hyperelliptic curve defined by

$$y^2 = (-1)^{n+1} \det(Q) \det(xI - T) = \text{disc}(Q) \det(xI - T).$$

To give a point on  $C$  is the same as giving a quadric in the pencil along with a choice of ruling. Let  $\tilde{C}$  denote its normalization. The geometric genus  $p_g$  of  $C$  is defined to be the genus of  $\tilde{C}$ . Let  $C^{sm}$  denote the smooth locus of  $C$ .

**Lemma 1.64.** If  $W$  is an  $n + 1$  dimensional subspace of  $U \otimes k^s$  isotropic with respect to  $Q_1, Q_2$ , then  $W$  is  $T$ -stable, where  $n \geq 0$ .

**Proof:** Take any  $\lambda \in k$  that is not an eigenvalue of  $T$ . Then  $W = W^{\perp_Q} = W^{\perp_{Q_\lambda}}$ . Hence, for any  $w \in W$ ,  $(T - \lambda)w \in W^{\perp_Q} = W$ . In other words,  $W$  is  $T$ -stable.  $\square$

**Proposition 1.65.** The base locus  $B$  contains no  $\mathbb{P}^n$  if and only if  $p_g \geq 0$ . When  $C$  is reducible, or equivalently  $p_g = -1$ , the base locus  $B$  contains a unique  $\mathbb{P}^n$ .

**Proof:** Without loss of generality, assume  $k$  is separably closed. Suppose  $W$  is an  $n + 1$  dimensional subspace of  $U$  such that  $\mathbb{P}W \subset B$ . The above lemma says  $W$  contains an eigenvector  $v$  of  $T$ . Since  $W$  is isotropic, the eigenvalue of  $v$  has multiplicity at least 2. One can now reduce the problem to  $\bar{U} = v^\perp/v$  and  $\bar{W}$  is  $n$ -dimensional. Applying the above lemma and reduction repeatedly until  $\dim \bar{U} = 2$  and  $\dim \bar{W} = 1$ . Apply the above lemma again, we see that  $\bar{T}$  has a repeated eigenvalue and hence all the generalized eigenspaces of  $T$  have even dimension which implies that  $C$  is reducible. Conversely when  $C$  is reducible,  $\bar{W}$  is the unique 1-dimensional eigenspace of  $\bar{T}$  hence proving uniqueness. Existence follows from running the argument backwards.  $\square$

Let  $F_0$  denote the following variety over  $k$ ,

$$F_0 = \{\mathbb{P}X \mid \dim \mathbb{P}X = n - 1, \mathbb{P}X \subset B\}.$$

In view of the above subsection, we impose an open condition and look at the following variety,

$$F = \{\mathbb{P}X \in F_0 \mid \text{Span}\{X, TX\} \text{ has no non-zero } T\text{-stable subspace}\}. \quad (1.12)$$

**Lemma 1.66.** Suppose  $p_g \geq 0$ , then

$$\begin{aligned} F &= \{\mathbb{P}X \in F_0 \mid X \not\subset v^\perp, \text{ for all singular points } [v] \in B\} \\ &= \{\mathbb{P}X \in F_0 \mid [v] \notin \mathbb{P}X, \text{ for all singular points } [v] \in B\}. \end{aligned}$$

**Proof:** Suppose  $\mathbb{P}X \in F$ . Let  $[v]$  be any singular point of  $B$ , since  $v$  is an eigenvector,  $v \notin X$ . If  $X \subset v^\perp$ , then  $\mathbb{P}(\text{Span}\{X, v\})$  is a  $\mathbb{P}^n$  contained in  $B$ , contradicting Proposition 1.65.

Conversely, suppose  $\mathbb{P}X \notin F$ , then  $v \in \text{Span}\{X, TX\}$  for some eigenvector  $v$  of  $T$ . Since  $X$  is a isotropic with respect to every quadric in the pencil, we see that  $v \in \text{Span}\{X, TX\} \subset X^\perp$  and hence  $X \subset v^\perp$ .

For the second equality, suppose first  $X \subset v^\perp$  for some singular  $[v] \in B$ . If  $v \notin X$ , then aftering reduction to  $v^\perp/v$ ,  $(X \cap v^\perp)/v$  has dimension  $n$  which contradicts Proposition 1.65. Hence  $v \in X$ . Conversely, if  $v \in X$ , then  $X \subset v^\perp$  as above.  $\square$

**Remark 1.67.** The main reason why  $F$  was defined as in (1.12) instead of the more conceptual ones in Lemma 1.66 is that there is still some interesting geometry when  $p_g = -1$  as we saw in the previous subsection, and in that case, (1.12) is the more appropriate definition.

**Theorem 1.68.** Suppose  $p_g \geq 0$  and  $C$  only has nodal singularities. Then there is a commutative algebraic group structure  $+_G$  defined over  $k$  on the disconnected variety

$$G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F'$$

such that,

1.  $G^0 = \underline{\text{Pic}}^0(C)$  with component group  $G/G^0 \simeq \mathbb{Z}/4\mathbb{Z}$ ,
2.  $F'$  is isomorphic to  $F$  as varieties via the inversion map  $-1_G$ ,
3. the group law extends that on  $H = \underline{\text{Pic}}(C)/\mathbb{Z}D_0 \simeq \underline{\text{Pic}}^0(C) \dot{\cup} \underline{\text{Pic}}^1(C)$  where  $D_0$  is the hyperelliptic class.

From now on, we assume that  $p_g \geq 0$ . Since the base locus contains no  $\mathbb{P}^n$ , one can define  $\tau : C \times F_0 \rightarrow F_0$  as in the generic case.

**Lemma 1.69.**  $\tau$  restricts to a morphism  $C^{sm} \times F \rightarrow F$ .

**Proof:** Recall that given a pair  $(c, \mathbb{P}X) \in C^{sm} \times F$ , there is a unique  $\mathbb{P}Y \simeq \mathbb{P}^n$  in the quadric and the ruling defined by  $c$ , then  $\tau(c, \mathbb{P}X)$  is the residual intersection of  $\mathbb{P}Y$  with the base locus. The claim here is that  $\tau(c, \mathbb{P}X) \in F$ . Suppose for a contradiction that  $\mathbb{P}X' := \tau(c, \mathbb{P}X) \in F_0 - F$ . Then by Lemma 1.66, there exists a singular point  $[v] \in B$  such that  $X' \subset v^\perp$ . Hence the linear space  $\text{Span}\{X', v\}$  is isotropic with respect to every quadric in the pencil. Proposition 1.65 implies that  $v \in X'$ . Since  $X$  and  $X'$  intersect at codimension 1 and  $v \notin X$ , we see that

$$\mathbb{P}Y = \text{Span}\{\mathbb{P}X, \tau(c, \mathbb{P}X)\} = \text{Span}\{\mathbb{P}X, [v]\}.$$

Since  $\mathbb{P}Y$  lies in the quadric  $Q_\alpha$  where  $\alpha$  is the eigenvalue of  $v$ , we see that  $c = (\alpha, 0) \notin C^{sm}$ . Contradiction.  $\square$

As in the generic case, one obtains an action of  $C^{sm}$  on  $F \dot{\cup} F'$ ,

$$\mathbb{P}X + (c) = -\tau(\bar{c})\mathbb{P}X, \quad -\mathbb{P}X + (c) = \tau(c)\mathbb{P}X. \quad (1.13)$$

This action extends to an action of  $\text{Div}(C^{sm})$  on  $F \dot{\cup} F'$ . To show that this descends to a simply-transitive action of  $\underline{\text{Pic}}^0(C)$ , we assume  $k = k^s$  and work over the algebraic closure. Let  $v$  be an eigenvector with eigenvalue  $\alpha$  of multiplicity  $m \geq 2$ . As usual, let  $(\bar{U}, \bar{Q})$  denote the

$2n$ -dimensional quadratic space  $v^\perp/v$ , let  $\overline{T}$  denote the descent of  $T$  to  $\overline{U}$ . Let  $\overline{C}$  denote the (possible singular) hyperelliptic curve

$$y^2 = \text{disc}(\overline{Q}) \det(xI - \overline{T}) = \text{disc}(Q) \det(xI - T)/(x - \alpha)^2.$$

Note  $\overline{C} \rightarrow C$  is a partial normalization of  $C$ . There is a natural inclusion  $\iota : C^{sm} \hookrightarrow \overline{C}^{sm}$ . Define  $\overline{F}$  and  $\overline{F}_0$  in the analogous way as  $F$  and  $F_0$ . Suppose  $\mathbb{P}X \in F$ , write  $\overline{X} = (X \cap v^\perp)/v$ . Lemma 1.66 implies that  $\overline{X}$  has the correct dimension. It is clear therefore  $\overline{X} \in \overline{F}_0$ .

**Lemma 1.70.**  $\text{Span}\{\overline{X}, \overline{TX}\}$  has no non-zero  $\overline{T}$ -stable subspace.

**Proof:** Note this is immediate when  $C$  has only nodal singularities for this reduction step kills the  $\alpha$ -generalized eigenspace and leaves the rest unchanged. In general, by Lemma 1.66, it suffices to show  $\overline{X}$  does not contain any singular point of  $\overline{B}$ . Let  $v' \in U$  be such that  $(T - \alpha)v' = v$ . Then  $\overline{X}$  could possibly contain a singular point of  $\overline{B}$  if  $m \geq 4$  and  $v' + cv \in X$  for some  $c \in k$ . The latter condition implies  $v = (T - \alpha)(v' + cv) \in X^\perp$  contradicting  $X \not\subseteq v^\perp$ .  $\square$

Denote this reduction step by  $\delta_v : F \rightarrow \overline{F}$ . We now have the following commutative diagram,

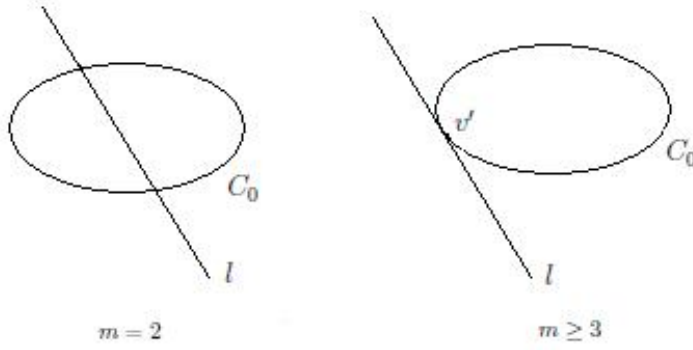
$$\begin{array}{ccc} C^{sm} \times F & \longrightarrow & F \\ \downarrow \iota \times \delta_v & & \downarrow \delta_v \\ \overline{C}^{sm} \times \overline{F} & \longrightarrow & \overline{F} \end{array}$$

The natural map  $\overline{C} \rightarrow C$  induces a map  $J(C) \rightarrow J(\overline{C})$  on their Jacobians with kernel either  $\mathbb{G}_m$  if the multiplicity  $m$  of  $\alpha$  is 2, or  $\mathbb{G}_a$  if  $m \geq 3$ . We now show that  $\delta_v$  is surjective and the preimage of every point is isomorphic to  $\ker(J(C) \rightarrow J(\overline{C}))$ . Let  $b_\alpha$  denote the bilinear form  $b_\alpha(u, u') = b(u, (T - \alpha)u')$  and by  $\perp_\alpha$  the operation of taking perpendicular space with respect to  $b_\alpha$ . Fix any  $\overline{X} \in \overline{F}$ . The bilinear form  $b_\alpha$  descends to a non-degenerate form on the  $2n + 1$

dimensional space  $U/v$ . Inside this space, we have

$$\begin{aligned}\dim \overline{X}^{\perp\alpha}/\overline{X} &= 3, \\ \dim (\overline{X}^{\perp\alpha} \cap v^{\perp})/\overline{X} &= 2.\end{aligned}$$

Stated in a different way,  $b_{\alpha}$  defines a smooth conic  $C_0$  in  $\mathbb{P}^2 = \mathbb{P}(\overline{X}^{\perp\alpha}/\overline{X})$  and  $l = \mathbb{P}((\overline{X}^{\perp\alpha} \cap v^{\perp})/\overline{X})$  is a line intersecting the conic at either one point or two points.



**Lemma 1.71.**  $l$  intersects  $C_0$  tangentially if and only if  $m \geq 3$ , in which case the point of intersection is  $[v' + \langle v \rangle + \overline{X}]$ , where  $v' \in U$  is such that  $(T - \alpha)v' = v$ .

**Proof:** Suppose  $l$  intersects  $C_0$  at a point  $w + \langle v \rangle + \overline{X}$ . To say  $l$  intersects  $C_0$  tangentially at  $w + \langle v \rangle + \overline{X}$  is equivalent to saying

$$w + \langle v \rangle \in \overline{X}^{\perp\alpha}, \quad b_{\alpha}(w, w) = 0, \quad w^{\perp\alpha} \cap \overline{X}^{\perp\alpha} = v^{\perp} \cap \overline{X}^{\perp\alpha}. \quad (1.14)$$

Since  $v'^{\perp\alpha} = v^{\perp}$ , we have  $v' \in (v^{\perp})^{\perp\alpha}$ . Thus  $(v^{\perp} \cap \overline{X}^{\perp\alpha})^{\perp\alpha} \cap \overline{X}^{\perp\alpha}$  is the line spanned by  $v' + \langle v \rangle$ . Since  $w \in (w^{\perp\alpha})^{\perp\alpha}$ , we see that up to scaling  $w + \langle v \rangle = v' + \langle v \rangle$ . Finally,  $b_{\alpha}(v', v') = b(v', v) = 0$  if and only if  $m \geq 3$ .

Conversely, suppose  $m \geq 3$ , then  $v' \in v^{\perp}$  and it is easy to see  $w = v'$  satisfies (1.14).  $\square$

Now given any point  $[w + \langle v \rangle + \overline{X}] \in C_0 - l$ , we can proceed to find a lift of  $\overline{X}$  to  $X^w \in F$

as follows. Since  $b(w, v) \neq 0$ , we can choose a lift of  $w \in U$  unique up to scaling such that  $b(w, w) = 0$  by adding an appropriate multiple of  $v$ , then take

$$X^w = \text{Span}\{w, u - \frac{b(w, u)}{b(w, v)}v\}_{u+\langle v \rangle \in \overline{X}} \subset U.$$

To check  $X^w \in F$ , we only need to check  $X^w \not\subset v^\perp$ , which is clear since  $b(w, v) \neq 0$ . For any two points in  $C_0 - l$ , the corresponding lifts to  $F$  are distinct as they have different images in  $U/v$ . Lastly, if  $X \in F$  such that  $\delta_v(X) = \overline{X}$ , then the image of  $X$  in  $U/v$  must be of the form  $\text{Span}\{\overline{X}, w + \langle v \rangle\}$  for some  $w + \langle v \rangle + \overline{X} \in C_0 - l$ . Therefore, we have prove the following proposition.

**Proposition 1.72.**  $\delta_v : F \rightarrow \overline{F}$  is surjective. The fibers are isomorphic to either (a conic minus a point)  $\simeq \mathbb{G}_a$  when  $m \geq 3$ , or (a conic minus two points)  $\simeq \mathbb{G}_m$  when  $m = 2$ . The kernel of the map  $J(C) \rightarrow J(\overline{C})$  has the same property.

One can now apply this reduction with any singular point of  $\overline{B}$  and so on. For each  $i$  such that  $m_i \geq 2$ , let  $v_{i,1}$  denote an eigenvector of  $T$  with eigenvalue  $m_i$ , and let  $v_{i,j}$  be such that  $(T - \alpha_i)v_{i,j} = v_{i,j-1}$  for  $j = 2, \dots, \lfloor \frac{m_i-1}{2} \rfloor$ . Let  $V$  denote the linear span of all such  $v_{i,j}$ . The above reduction will terminate at the  $2p_g + 2$  dimensional vector space  $\tilde{U} = V^\perp/V$ . The data  $(Q, T)$  descends to  $(\tilde{Q}, \tilde{T})$  on the  $2p_g + 2$  dimensional vector space  $\tilde{U} = V^\perp/V$  with  $\tilde{T}$  regular semi-simple. Let  $\tilde{F}$  denote the variety of (linear)  $p_g$ -dimensional common isotropic subspaces  $\tilde{X} \subset \tilde{U}$ . Let  $\delta : F \rightarrow \tilde{F}$  denote the composite of all the reductions. The associated smooth hyperelliptic curve  $\tilde{C}$  is the normalization of  $C$ . Note that if  $k$  is arbitrary, then  $V$  is defined over  $k$  and the composite  $\delta$  is defined over  $k$ . We summarize the above discussion into the following Theorem.

**Theorem 1.73.** Suppose  $p_g \geq 0$  and  $k$  is algebraically closed. Then:

1. The map  $\delta : F \rightarrow \tilde{F}$  is surjective. The pre-image of every point has a filtration with  $\mathbb{G}_a$  and  $\mathbb{G}_m$  factors. The kernel of the natural map  $J(C) \rightarrow J(\tilde{C})$  has a filtration with the same factors.

2. There is an action of  $\text{Div}^0(C^{sm})$  on  $F$  that descends to the simply-transitive action of  $J(\tilde{C})$  on  $\tilde{F}$ .

Therefore to prove Theorem 1.68, it remains to show that the action of  $\text{Div}(C^{sm})$  on  $F \dot{\cup} F'$  descends to a simply-transitive action of  $\text{Pic}(C)$  on  $F \dot{\cup} F'$ . Once again we pass to the algebraic closure and use the same formal argument as in the generic case. We list the “non-formal” results one needs to verify in the regular case.

1. Lemma 1.20, which allows one to define the  $\infty$ -minimal form of a divisor class  $[D] \in J(C)$  and hence a morphism  $\varphi : J \rightarrow \text{Aut}(F)$ . Here we need to assume that  $C$  has a smooth Weierstrass point.
2. Show  $\varphi$  is a group homomorphism, to conclude that principal divisors supported on  $C^{sm}$  act trivially on  $F \dot{\cup} F'$ .
3. The existence part of Lemma 1.19, to conclude that the action of  $J$  on  $F$  is transitive.
4. The uniqueness part of Lemma 1.19, to conclude that the action is simply-transitive.

Lemma 1.20 still holds in the singular case because Riemann-Roch holds in the singular case ([10]). Suppose  $C$  has a smooth Weierstrass point  $\infty$ , which it always has if  $C$  only has nodal singularity and  $p_g \geq 0$ . Every class  $[D] \in J(C)$  has a  $\infty$ -minimal form  $[D' - r(\infty)]$  where  $D'$  is effective of degree  $r \geq n$  supported on  $C^{sm}$  and  $h^0(D) = 1$ . This allows us to define a morphism of varieties  $\varphi : J \rightarrow \text{Aut}(F)$ . The image of  $\varphi$  lies in a commutative subvariety of  $\text{Aut}(F)$ .

We now specialize to the case where  $C$  only has nodal singularities, so  $J$  is an extension of an abelian variety  $\tilde{J}$  of dimension  $p_g$  by an  $n - p_g$  dimensional torus  $S$ .

**Lemma 1.74.**  $\varphi$  is a morphism of algebraic groups.

**Proof:** The proof is very similar to the proof that a morphism between semi-abelian varieties mapping the identity to the identity is a group homomorphism. For any  $s \in S$ , its image in  $\tilde{J}$  is



0, hence it acts on the fibers of the map  $\delta : F \rightarrow \tilde{F}$  which are also tori. Therefore  $\varphi|_S$  is a group homomorphism. For any  $a \in J$ , we define  $\varphi_a : S \rightarrow \text{Aut}(F)$  by

$$\varphi_a(s) = \varphi(a)\varphi(s)\varphi(as)^{-1}.$$

Fix any  $x \in F$ , we have  $\delta(x) = \delta(\varphi_a(s)(x))$ . Let  $S'$  denote the fiber of  $\delta$  over  $\delta(x)$ , we have thus defined a map  $\varphi_{a,x} : S \rightarrow S'$  between tori, which is automatically a group homomorphism. Letting  $a$  vary, one obtains a map  $\varphi_x : J \rightarrow \text{End}(S, S')$ . Since  $J$  is connected and  $\text{End}(S, S')$  is discrete,  $\varphi_x$  is constant. Taking any  $s \in S$ , we see  $\varphi_x(a) = \varphi_x(s)$  is the trivial map  $S \rightarrow S'$ . Letting  $x$  vary, we have proved that

$$\varphi(a)\varphi(s) = \varphi(as), \quad \forall a \in J, s \in S. \quad (1.15)$$

Now fix  $a \in J$  and view  $\varphi_a$  as a morphism  $J \rightarrow \text{Aut}(F)$ . Since  $\varphi_a$  vanishes on  $S$  and (1.15) allows us to descend  $\varphi_a$  to a morphism  $\tilde{J} \rightarrow \text{Aut}(F)$ . Once again, fixing any  $x \in F$ ,  $\varphi_a(a')$  acts on the fiber over  $\delta(x)$ . Hence we have a morphism  $\varphi_{a,x} : \tilde{J} \rightarrow S'$  which is trivial since  $\tilde{J}$  is an abelian variety and  $S'$  is a torus. Letting  $x$  vary, one sees that  $\varphi_a$  is trivial. Letting  $a$  vary gives the desired result.  $\square$

As in the proof of Proposition 1.17, we have shown that principal divisors supported on  $C^{sm}$  act trivially on  $F \dot{\cup} F'$ . Next we show transitivity of this action. Since  $\text{Div}(C^{sm})$  also acts on  $F_0 \dot{\cup} F'_0$  and  $F \dot{\cup} F'$  is open in  $F_0 \dot{\cup} F'_0$ , by taking Zariski closure one sees that principal divisors supported on  $C^{sm}$  act trivially on  $F_0 \dot{\cup} F'_0$ . Since being supported on  $C^{sm}$  is also an open condition, one also has that principal divisors on  $C$  act trivially on  $F_0$ . The existence part of Lemma 1.19 can be applied to  $F_0$  since the defining map  $C \rightarrow \mathbb{P}^1$  admits no section. In other words, given  $x, x' \in F$ , view them as in  $F_0$  where there exists an effective divisor  $D \in \text{Div}(C)$  such that  $x + D = \pm x'$ . Let  $D'$  be a divisor supported on  $C^{sm}$  linearly equivalent to  $D$ . Since principal divisors on  $C$  act trivially,  $x + D' = x + D = \pm x'$ . Transitivity then follows from the formal argument in the proof of Proposition 1.16. Note here the existence of a smooth

Weierstrass point is needed because we need to know there exists  $\mathbb{P}X \in F$  such that  $T_{\mathbb{P}X}B \simeq \mathbb{P}^n$ .

The uniqueness part of Lemma 1.19 also holds for  $F_0$ . The argument in [7] works since there is no injective map from  $\mathbb{P}^1$  to  $C$  when the arithmetic genus  $n$  of  $C$  is at least 1. The same formal argument in the generic case then implies that only principal divisors act trivially. Note that for the proof of Lemma 1.25, it is important there is a smooth Weierstrass point  $\infty$  for we need to know that there are finitely many element of  $F$  fixed by  $\tau(\infty)$ . The following result is immediate from Theorem 1.68 and Theorem 1.73.

**Corollary 1.75.** Suppose  $p_g \geq 0$  and  $C$  only has nodal singularities. Then the short exact sequence

$$1 \rightarrow T \rightarrow J(C) \rightarrow J(\tilde{C}) \rightarrow 1$$

extends to a short exact sequence

$$1 \rightarrow T \rightarrow G \rightarrow \tilde{G} \rightarrow 1,$$

where  $G = \underline{\text{Pic}}^0(C) \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F'$  and  $\tilde{G} = \underline{\text{Pic}}^0(\tilde{C}) \dot{\cup} \tilde{F} \dot{\cup} \underline{\text{Pic}}^1(\tilde{C}) \dot{\cup} \tilde{F}'$  are the corresponding disconnected groups of four components.

Now over the algebraic closure, after identifying  $F$  with  $J(C)$ , one can obtain a compactification of  $J(C)$  by taking  $F_0$ . Recall for any singular  $[v] \in B$ , we have the reduction map  $\delta_v : F_0 \rightarrow \overline{F}_0$ . Note this map might not be a morphism. The composition of all the reduction map gives  $\delta : F_0 \rightarrow \tilde{F} \simeq J(\tilde{C})$ . Each fiber of  $\delta_v$  intersects  $F_0 \setminus F$  at one point, obtained by taking the preimage of  $\mathbb{P}X \in \overline{F}_0$  under the map  $v^\perp \rightarrow v^\perp/v$ .

**Corollary 1.76.** Suppose  $p_g \geq 0$  and  $C$  has only nodal singularities, then  $F_0$  is a compactification of  $J(C)$  by adding one point to each  $\mathbb{G}_m$  factor of the fiber over  $J(\tilde{C})$ .

We expect that the condition on  $C$  having only nodal singularities is unnecessary. If Theorem 1.68 is proved without this condition, then Corollary 1.76 also holds without this condition. The compactification  $F_0$  is not smooth.

## 2 Principal homogeneous spaces of Jacobians

In this chapter, we will use the geometric theory obtained in the previous chapter to obtain a correspondence between the problem of 2-descent on Jacobian of hyperelliptic curves over  $k$  and the study of certain  $k$ -orbits of the natural PO or PSO action on self-adjoint operators. We keep the assumption that the characteristic of  $k$  is not 2. All polynomials are assumed to split completely over the separable closure.

### 2.1 Weil's viewpoint

The idea of studying torsors  $F$  of abelian varieties  $J$  of order  $n$  by studying a disconnected algebraic group

$$G = J \dot{\cup} F \dot{\cup} F^2 \dot{\cup} \dots \dot{\cup} F^{n-1} \quad (2.1)$$

was originally due to André Weil. Knowing the class  $[F] \in H^1(k, J)[n]$  gives rise to a  $J$ -equivariant from  $n$  copies of  $F$  to  $J$ ,

$$f : F \times \dots \times F \rightarrow J, \quad (2.2)$$

unique up to post-composition by translation by some  $[D] \in J(k)$ . Here  $J$ -equivariance means that for  $X_1, \dots, X_n \in F$  and  $[D_1], \dots, [D_n] \in J$ ,

$$f(X_1 + [D_1], \dots, X_n + [D_n]) = f(X_1, \dots, X_n) + [D_1] + \dots + [D_n].$$

Knowing the group  $G$ , on the other hand, pins down this choice.

Suppose  $(\text{char}(k), n) = 1$ , so that multiplication by  $n$  is surjective on  $J(k^s)$ . One has the following descent exact sequence

$$0 \rightarrow J(k)/nJ(k) \xrightarrow{\delta} H^1(k, J[n]) \rightarrow H^1(k, J)[n] \rightarrow 0. \quad (2.3)$$

There is a very simple relationship between the choice of  $f$  in (2.2) and the choice of a lift of  $[F]$  to a torsor of  $J[n]$ . Namely, define

$$F[n]_f = \{x \in F \mid f(x, x, \dots, x) = 0\}.$$

The assumption of the characteristic of  $k$  implies that  $F[n]_f(k^s)$  is non-empty. Furthermore, it is clear from the definition that  $F[n]_f$  is a torsor of  $J[n]$  and it maps to  $[F]$  in  $H^1(k, J)[n]$ .

If one post-composes  $f$  by translation by  $[D] \in J(k)$  and call the new map  $f + [D]$ , then again by definition,

$$[F[n]_{f+[D]}] = [F[n]_f] + \delta([D]) \in H^1(k, J[n]).$$

Two maps  $f_1, f_2$  are **equivalent** if they differ by some  $[D] \in nJ(k)$ . This notion of equivalence is the same as the usual equivalence among morphisms of torsors.

**Proposition 2.1.** There is a bijection between equivalence classes of  $J$ -equivariant morphisms  $f : F \times \dots \times F \rightarrow J$  and lifts of  $[F]$  to torsors of  $J[n]$ .

If moreover one has the datum of the disconnected group  $G$  as in (2.1), then one has a specific  $f$  and a specific lift. Namely

$$F[n]_0 := \{x \in F \mid nx = 0 \in G\}.$$

All the other lifts are given by

$$F[n]_{[D]} = \{x \in F \mid nx = [D] \in G\}$$

for  $[D] \in J(k)$ . Two lifts  $F[n]_{[D_1]}, F[n]_{[D_2]}$  are equivalent if and only if  $[D_1] = [D_2] \pmod{nJ(k)}$ .

## 2.2 Pencil of quadrics containing a rational singular quadric

Let  $U$  be a vector space over  $k$  of dimension  $2n + 2$ . Let  $\mathcal{L}(Q_1, Q_2)$  be a rational generic pencil in  $\mathbb{P}^{2n+1} = \mathbb{P}U$  with associated hyperelliptic curve

$$C : y^2 = f(x) = (-1)^{n+1} \det(xQ_1 - Q_2).$$

Note  $C$  has a rational Weierstrass point if and only if  $f(x)$  has a root over  $k$  if and only if one of the rational quadrics in  $\mathcal{L}$  is singular. In this section, we assume such is the case, and by moving this point to  $\infty$ , we assume that  $Q_1$  is singular and that  $f(x)$  has odd degree. Denote the cone point of  $Q_1$  by  $[v_\infty]$  for some  $v_\infty \in U$ . Let  $J$  denote the Jacobian of  $C$ .

Let  $F$  denote the variety of  $(n-1)$ -planes contained in the base locus  $B = Q_1 \cap Q_2$ . Theorem 1.27 shows that  $F$  fits inside a disconnected algebraic group over  $k$ ,

$$G = J \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F'.$$

Since  $\underline{\text{Pic}}^1(C)$  has a point, namely  $(\infty)$ , we can lift  $[F] \in H^1(k, J)[2]$  to a torsor of  $J[2]$  via

$$F[2]_\infty = \{\mathbb{P}X \in F \mid \mathbb{P}X +_G \mathbb{P}X = (\infty)\} = \{\mathbb{P}X \in F \mid \mathbb{P}X = \tau(\infty)\mathbb{P}X\}.$$

**Proposition 2.2.** Let  $H = v_\infty^{\perp Q_2}$  be the hyperplane in  $U$  orthogonal to  $v_\infty$  with respect to  $Q_2$ . Then

$$F[2]_\infty = \{\mathbb{P}X \mid \mathbb{P}X \subset B \cap \mathbb{P}H, \dim(\mathbb{P}X) = n-1\} \subset \mathbb{G}r(n-1, \mathbb{P}H).$$

**Proof:** Note  $H$  is independent of the choice of  $Q_2 \in \mathcal{L}(k)$ , so we assume without loss of generality that  $Q_2$  is nonsingular. Let  $[v_P]$  denote the cone point of the singular quadric corresponding to the Weierstrass point  $P \in C(k^s)$ . Let  $b_2$  denote the associated bilinear form of  $Q_2$ . Genericness forces  $b_2(v_P, v_P) \neq 0$ .

To compute  $\tau(P)\mathbb{P}X$  for  $\mathbb{P}X \in F(k^a)$ , one takes the  $n$ -plane spanned by  $\mathbb{P}X$  and  $[v_P]$  and takes its residue intersection with  $Q_2$ . As we saw in the definition of  $\tau$  in Section 1.2, the action

of  $\tau(P)$  on  $F$  is induced by the following map on  $U \otimes k^a$  :

$$\text{refl}_P : x \mapsto x - 2 \frac{b_2(x, v_p)}{b_2(v_p, v_p)} v_p, \quad (2.4)$$

and hence

$$\{\mathbb{P}X \in F(k^a) | \mathbb{P}X = \tau(P)\mathbb{P}X\} = \{\mathbb{P}X \simeq \mathbb{P}_{k^a}^{n-1} | \mathbb{P}X \subset B \cap \mathbb{P}v_P^{\perp Q_2}\}.$$

When  $v_P$  is  $k$ -rational,  $\text{refl}_P$  and  $v_P^{\perp Q_2}$  are defined over  $k$  and we obtain the desired result.  $\square$

**Remark 2.3.** Since  $f$  has no repeated factors,  $\mathcal{L} \cap H$  is a rational generic pencil of quadrics in  $\mathbb{P}^{2n}$ . We have seen in Section 1.1 that if  $Q_1$  restricted to  $H$  is split, then the variety of  $(n-1)$ -planes contained in the base locus of  $\mathcal{L} \cap H$  forms a principal homogeneous space for  $J[2]$ . We will see later that the two torsors of  $J[2]$  coincide.

## 2.3 Orbits of an action of $\text{PO}_{2n+1}$

Suppose now  $(U_0, Q_0)$  is a  $2n+1$  dimensional orthogonal space over  $k$ . We would like to study the orbits of the conjugation action of  $\text{PO}(U_0, Q_0)$  on  $V_f$ , the space of self-adjoint operators  $T$  on  $U_0$  with fixed characteristic polynomial  $f(x)$ . We also assume  $f(x)$  has no repeated roots.

We have seen in Proposition 1.1 that there is only one geometric orbit, that is over the separable closure, self-adjoint operators with the same characteristic polynomial are conjugate to each other by an element of  $\text{PO}(U_0, Q_0)(k^s)$ . The goal of this section and the next is to study how this one geometric orbit decomposes over the base field  $k$ .

Since multiplying  $Q_0$  by a constant in  $k^\times$  does not change  $V_f$  or  $\text{PO}(U_0, Q_0)$ , we assume without loss of generality that  $Q_0$  has discriminant 1. As pointed out in Section 1.1,  $V_f(k)$  could be empty in general. Hence in what follows,  $Q_0$  is assumed to be split, and we write  $\text{PO}_{2n+1}$  for  $\text{PO}(U_0, Q_0)$ .

Fix any  $(T_0, X_0) \in W_f(k)$ , which is also nonempty by Lemma 1.2, the  $\text{PO}_{2n+1}(k)$ -orbits of

$V_f(k)$  are in bijection with

$$\ker \left( H^1(k, \text{Stab}(T_0)) \rightarrow H^1(k, \text{PO}_{2n+1}) \right). \quad (2.5)$$

Let  $C$  be the hyperelliptic curve defined by  $y^2 = f(x)$  and  $J$  its Jacobian. By Corollary 1.5, for each  $T \in V_f(k)$ , one can identify  $\text{Stab}(T)$  with  $J[2]$  and obtain a class  $c_T$  in  $H^1(k, J[2])$  by taking

$$W_T = \{X | (T, X) \in W_f\}.$$

**Lemma 2.4.** The map

$$\text{PO}_{2n+1}(k) \backslash V_f(k) \rightarrow \ker \left( H^1(k, J[2]) \rightarrow H^1(k, \text{PO}_{2n+1}) \right)$$

is given by  $T \mapsto c_T$ .

**Proof:** Fix any  $T \in V_f(k)$ , suppose  $g \in \text{PO}_{2n+1}(k^s)$  sends  $T_0$  to  $T$ . The class in  $H^1(k, \text{Stab}(T_0))$  corresponding to the orbit of  $T$  is  $(g^{-1}\sigma g)_\sigma$ . Set  $X = gX_0$ . The class in  $H^1(k, \text{Stab}(T))$  corresponding to  $W_T$  is  $(\sigma g g^{-1})_\sigma$  for it is the element in  $\text{Stab}(T)$  sending  $X$  to  $\sigma X$ . These two classes have the same image in  $H^1(k, J[2])$  because the composite map

$$\text{Stab}(T_0) \simeq J[2] \simeq \text{Stab}(T)$$

is induced by the conjugation by  $g$  map on  $\text{PO}_{2n+1}$ . □

The **distinguished** orbit corresponds to the trivial class in  $H^1(k, J[2])$ . It consists of self-adjoint operators  $T$  such that  $W_T(k) \neq \emptyset$ , namely there exists a linear  $n$ -dimensional subspace  $X \subset U$  defined over  $k$  such that  $X \subset X^\perp, TX \subset X^\perp$ .

There is another special collection of orbits. Let  $b$  denote the bilinear form associated to  $Q_0$ . For any  $T \in V_f(k)$ , consider the  $2n + 2$  dimensional vector space  $U = U_0 \oplus k$  with the following

two quadratic forms

$$\begin{aligned} Q(v, w) &= b(v, v) \\ Q_T(v, w) &= b(v, Tv) + w^2. \end{aligned}$$

Let  $F_T$  denote the following variety:

$$F_T = \{\mathbb{P}X \mid \dim(\mathbb{P}X) = n - 1, X \subset X^{\perp_Q}, X \subset X^{\perp_{Q_T}}\} \subset \mathbb{G}r(n - 1, \mathbb{P}U).$$

The **soluble** orbits are the  $\mathrm{PO}_{2n+1}(k)$ -orbits of self-adjoint operators  $T$  for which  $F_T(k) \neq \emptyset$ .

**Theorem 2.5.** The soluble orbits correspond bijectively to the image of  $J(k)/2J(k)$  in  $H^1(k, J[2])$ .

In particular, the composition

$$J(k)/2J(k) \xrightarrow{\delta} H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PO}_{2n+1})$$

is trivial.

In this section we will only show that the soluble orbits lands inside  $\delta(J(k)/2J(k))$ . Surjectivity will be proved in the next section after a 2-descent analysis on  $J$ .

**Lemma 2.6.** The pencil of quadrics spanned by  $Q, Q_T$  in  $\mathbb{P}(U)$  is rational generic.

**Proof:** Rationality is clear. Genericness follows from the following computation.

$$\begin{aligned} (-1)^{n+1} \det(xQ - Q_T) &= (-1)^{n+1} \det(b) \det(xI - T) \cdot (-1) \\ &= (-1)^n \det(b) f(x) \\ &= f(x). \end{aligned}$$

If we denote the roots of  $f$  over  $k^s$  by  $\alpha_1, \dots, \alpha_{2n+2}$ , the  $2n + 2$  singular quadrics in the pencil are  $Q, \alpha_1 Q - Q_T, \dots, \alpha_{2n+1} Q - Q_T$ . □



The hyperelliptic curve associated to the pencil is defined by the affine equation

$$y^2 = (-1)^{n+1} \det(xQ - Q_T) = f(x),$$

which is the same as the curve  $C$  defined above. The pencil contains a rational singular quadric  $Q$  and the curve  $C$  has a rational Weierstrass point  $\infty$ . Therefore we are in the situation in Section 2.2 and  $F_T$  is a torsor for  $J$  of order dividing 2.

The cone point of  $Q$  is  $[v_\infty] = [0, \dots, 0, 1]$ . The hyperplane  $\mathbb{P}H = \mathbb{P}(v_\infty^\perp)$  is  $\mathbb{P}(U_0)$ . Hence by Proposition 2.2,  $F_T[2]_\infty = W_T$  as  $\text{Gal}(k^s/k)$ -sets, in the sense

$$F_T[2]_\infty = \{\mathbb{P}X \mid X \in W_T\}. \quad (2.6)$$

**Proposition 2.7.**  $F_T[2]_\infty = W_T$  as  $J[2]$ -torsors. Therefore

$$[F_T[2]_\infty] = c_T \in H^1(k, J[2]).$$

**Proof:** It suffices to show for any  $(P) - (\infty) \in J[2](k^s)$  with  $P$  a Weierstrass point, the two actions are the same. Let  $\alpha$  denote the root of  $f(x)$  corresponding to  $P$ , and set  $h(x) = f(x)/(x - \alpha)$ . On  $W_T(k^s)$ , by Remark 1.6, the action of  $(P) - (\infty)$  is induced by the following map on  $U_0 \otimes k^s$ :

$$x \mapsto x - 2 \frac{h(T)}{h(\alpha)} x.$$

We now compute the action of  $(P) - (\infty)$  on  $F_T[2]_\infty(k^s)$ . The singular quadric corresponding to  $P$  is  $\alpha Q - Q_T$ . Let  $w_P \in U_0 \otimes k^s$  be an eigenvector of  $T$  with eigenvalue  $\alpha$ . The cone point of  $\alpha Q - Q_T$  is  $[(w_P, 0)]$ . Let  $b_T$  denote bilinear form associated to  $Q_T$ . From the definition of  $\tau$  in Section 1.2, we see that the action of  $(P) - (\infty)$  is induced by the following map on  $U \otimes k^s$ :

$$x \mapsto x - 2 \frac{b_T(x, (w_P, 0))}{b_T((w_P, 0), (w_P, 0))} (w_P, 0).$$

If we view each  $\mathbb{P}X \in F_T[2]_\infty(k^s)$  as sitting inside  $\mathbb{P}(U_0)$ , then the action of  $(P) - (\infty)$  is induced by the following map on  $U_0 \otimes k^s$  :

$$x \mapsto x - 2 \frac{b(x, w_P)}{b(w_P, w_P)} w_P.$$

To prove the lemma, it remains to show for any  $x \in U_0 \otimes k^s$ ,

$$\frac{h(T)}{h(\alpha)} x = \frac{b(x, w_P)}{b(w_P, w_P)} w_P.$$

Since both sides are killed by  $T - \alpha$ , and since  $T$  has 1-dimensional eigenspaces, they are both scalar multiples of  $w_P$ . Now

$$b\left(\frac{h(T)}{h(\alpha)} x, w_P\right) = b\left(x, \frac{h(T)}{h(\alpha)} w_P\right) = b(x, w_P) = b\left(\frac{b(x, w_P)}{b(w_P, w_P)} w_P, w_P\right).$$

Therefore they are the same scalar multiple of  $w_P$ . □

**Remark 2.8.** Equation (2.6) offers another view point for the canonical identification of  $J[2]$  with the stabilizer of a self-adjoint operator, namely they share a common principal homogeneous space. Fix any  $k$ -rational  $T$ , then  $J[2]$  acts on  $F[2]_\infty$  simply-transitively and  $\text{Stab}(T)$  acts on  $W_T$  simply-transitively. It is clear from the definitions that these two actions commute. Fix some  $X_0 \in F[2]_\infty$ , one can define the map

$$\iota : J[2] \rightarrow \text{Stab}(T)$$

by taking  $\iota([D])$ , for any  $[D] \in J[2]$ , to be the unique element of  $\text{Stab}(T)$  sending  $X_0$  to  $X_0 + [D]$ . Commutativity of the two actions and commutativity of  $J[2]$  show that this map is independent on the choice of  $X_0$ . Proposition 2.7 then implies that  $\iota$  is given by the map we defined in Remark 1.6.

**Corollary 2.9.** The composite map

$$\mathrm{PO}_{2n+1}(k) \backslash V_f(k) \rightarrow H^1(k, J[2]) \rightarrow H^1(k, J)[2]$$

is given by  $T \mapsto [F_T]$ .

**Corollary 2.10.** The soluble orbits map into the image of  $J(k)/2J(k)$  in  $H^1(k, J[2])$ . The correspondence is given by  $T \mapsto c_T = \delta(\mathbb{P}X +_G \mathbb{P}X - (\infty))$  for any  $\mathbb{P}X \in F_T(k)$ , where  $+_G$  is the addition law on  $G = J \dot{\cup} F_T \dot{\cup} \underline{\mathrm{Pic}}^1(C) \dot{\cup} F'_T$  as in Theorem 1.27.

**Proof:** The first claim is immediate from the definition of soluble orbits. Suppose  $T \in V_f(k)$  is soluble and suppose  $[F_T[2]_\infty] = \delta([D])$  for  $[D] \in J(k)$ . Let  $X_0 \in F_T[2](k^s)$  and  $[E] \in J(k^s)$  such that  $[D] = 2[E]$  and

$$X_0 + X_0 = (\infty), \quad {}^\sigma X_0 - X_0 = \delta([D]) = {}^\sigma[E] - [E].$$

Then  $X_0 - [E] \in F_T(k)$  and

$$2(X_0 - [E]) - (\infty) = -[D] = [D] \pmod{2J(k)}. \quad \square$$

## 2.4 Hyperelliptic curves with a rational Weierstrass point

In this section we aim to complete the proof of Theorem 2.5.

Let  $C$  be a hyperelliptic curve of genus  $n$  with a rational Weierstrass point, let  $J$  denote its Jacobian. By moving the point to  $\infty$ , we can assume  $C$  is given by affine equation  $y^2 = f(x)$  where  $f(x)$  is a monic degree  $2n+1$  polynomial. Let  $P_1, \dots, P_{2n+1}, \infty$  denote the  $2n+2$  Weierstrass points. Then

$$J[2](k^s) = \langle (P_i) - (\infty) \mid \sum_{i=1}^{2n+1} ((P_i) - (\infty)) = \mathrm{div}(y) = 0 \rangle \quad (2.7)$$

is an elementary 2-group of order  $2^{2n}$ . As a group scheme over  $k$ ,

$$J[2] = \text{Res}_{L/k} \mu_2 / \mu_2 \simeq (\text{Res}_{L/k} \mu_2)_{N=1}$$

where  $L = k[x]/f(x) = k[\beta]$  is an étale  $k$ -algebra of dimension  $2n + 1$ . From the exact sequence

$$1 \rightarrow (\text{Res}_{L/k} \mu_2)_{N=1} \rightarrow \text{Res}_{L/k} \mu_2 \xrightarrow{N} \mu_2 \rightarrow 1,$$

one gets by taking cohomology,

$$H^1(k, J[2]) = (L^\times / L^{\times 2})_{N=1}. \quad (2.8)$$

Take any  $\alpha \in (L^\times / L^{\times 2})_{N=1}$ , we will first construct a torsor for  $J$  using pencils of quadrics such that its canonical lift to a torsor of  $J[2]$  recovers the class  $\alpha$ . Then we will show when  $\alpha$  lies in the image of  $J(k)/2J(k)$ , there is a soluble orbit corresponding to it.

Lift  $\alpha$  to an element in  $L^\times$  whose norm to  $k$  is a square. Denote the lift by  $\alpha$  also. Let  $\sqrt{\alpha}$  denote a square root of  $\alpha$  in  $L \otimes k^s$ . Then the identification in (2.8) is given by

$$\alpha \mapsto \left( \frac{\sigma \sqrt{\alpha}}{\sqrt{\alpha}} \right)_\sigma \in H^1(\text{Gal}(k^s/k), \mu_2(L \otimes k^s)_{N=1}^\times).$$

Consider the quadric  $Q_0$  on  $L$  defined by the bilinear form

$$\langle \lambda, \mu \rangle_\alpha = \text{coefficient of } \beta^{2n} \text{ in } \alpha \lambda \mu.$$

Since  $N_{L/k}(\alpha)$  is a square in  $k$ ,  $Q_0$  has discriminant 1. Choosing a different lift of  $\alpha$  does not change the  $k$ -isomorphism type of  $Q_0$ . Let  $T$  denote the multiplication by  $\beta$  operator, note  $T$  is self-adjoint with respect to  $Q_0$ . Let  $X_0$  be the following  $n$ -dimensional  $k^s$ -subspace of  $L \otimes k^s$  :

$$X_0 = \text{Span}_{k^s} \left\{ \frac{1}{\sqrt{\alpha}}, \frac{\beta}{\sqrt{\alpha}}, \dots, \frac{\beta^{n-1}}{\sqrt{\alpha}} \right\}.$$

Since  $T$  is  $k$ -rational, we can still use much of the theory in Section 2.3 even though a priori  $Q_0$  might not be split. On  $\mathbb{P}(L \oplus k)$ , there is a rational generic pencil of quadrics spanned by  $Q, Q_T$  given by the following formula in terms of quadratic forms:

$$\begin{aligned} Q(v, w) &= \langle v, v \rangle_\alpha \\ Q_T(v, w) &= \langle v, \beta v \rangle_\alpha + w^2. \end{aligned}$$

Since  $Q_0$  has discriminant 1 and  $T$  has characteristic polynomial  $f(x)$ , the hyperelliptic curve associated to this pencil is  $C$ . Taking the variety  $F_T$  of  $(n-1)$ -planes in the base locus of this pencil in  $\mathbb{P}(L \oplus k)$  gives a torsor of  $J$  of order dividing 2.

**Proposition 2.11.** Its canonical lift  $[F_T[2]_\infty] \in H^1(k, J[2])$  recovers  $\alpha$ . In particular, all torsors of  $J[2]$  arise from pencils of quadrics.

**Proof:** Since  $X_0 \in W_T(k^s) = F_T[2]_\infty(k^s)$  and

$${}^\sigma X_0 = \frac{{}^\sigma \sqrt{\alpha}}{\sqrt{\alpha}} X_0$$

for all  $\sigma \in \text{Gal}(k^s/k)$ . We see that  ${}^\sigma \sqrt{\alpha}/\sqrt{\alpha}$  is the element of  $\text{Stab}(T)$  sending  $X_0$  to  ${}^\sigma X_0$ . By Proposition 2.7,  $F_T[2]_\infty = W_T$  as  $J[2]$ -torsors. Hence,  ${}^\sigma \sqrt{\alpha}/\sqrt{\alpha}$  is also the element of  $J[2]$  sending  $X_0$  to  ${}^\sigma X_0$  viewed as elements of  $F_T[2]_\infty$ .  $\square$

Suppose now  $\alpha$  lies in the image of  $J(k)/2J(k)$ , then  $F_T$  is the trivial torsor. Take any  $\mathbb{P}X \in F_T(k)$ , just as in the proof of Corollary 2.10,  $\mathbb{P}X +_G \mathbb{P}X - (\infty)$  recovers this class in  $J(k)/2J(k)$ . See Section 2.10 for some a different proof of this by explicitly writing down a rational  $\mathbb{P}X$  and calculating  $\mathbb{P}X +_G \mathbb{P}X$ .

Since  $X$  is an  $n$ -dimensional  $k$ -subspace of  $L \oplus k$  isotropic with respect to  $Q_T$ , we see that the projection of  $X$  to  $L$  is again  $n$ -dimensional. Therefore  $Q_0$  is split of discriminant 1. Fix any isometry between  $L$  and the orthogonal space  $U_0$  defined in Section 2.3, and let  $T' \in V_f(k)$  denote the image of  $T$ . Any two isometries differ by an element  $g$  of  $O_{2n+1}(k)$ , and it changes  $T'$

by conjugation by  $g$ . As the center of  $O_{2n+1}(k)$  acts trivially on  $V_f(k)$ , we obtain a well-defined  $O_{2n+1}(k)/(\pm 1) = \text{PO}_{2n+1}(k)$ -orbit of  $k$ -rational self-adjoint operators. This orbit is soluble by construction and its class in  $H^1(k, J[2])$  is,

$$c_{T'} = c_T = \alpha.$$

Hence we have established the surjectivity in Theorem 2.5, which we will state again for completeness.

**Theorem 2.12.** There is a bijection between  $J(k)/2J(k)$  and soluble orbits of self-adjoint operators with characteristic polynomial  $f(x)$ .

In fact, we can also describe all the other  $\text{PO}_{2n+1}(k)$ -orbits. The above identification of  $L$  with  $U_0$  only required the splitness of  $<, >_\alpha$ . Once we know  $<, >_\alpha$  is split, the image of  $T$  under the identification gives us a  $\text{PO}_{2n+1}(k)$ -orbit whose class in  $H^1(k, J[2])$  is  $\alpha$ .

**Proposition 2.13.** For  $\alpha \in (L^\times/L^{\times 2})_{N=1}$ ,  $<, >_\alpha$  is split if and only if  $\alpha$  lies in

$$\ker(H^1(k, J[2]) \rightarrow H^1(k, \text{PO}_{2n+1})).$$

**Proof:** The heuristic here is that the image of  $\alpha$  in  $H^1(k, \text{PO}_{2n+1}) = H^1(k, \text{SO}_{2n+1})$  is the class corresponding to the form  $<, >_\alpha$ , hence is trivial if and only if  $<, >_\alpha$  is split. Rigorously, choose  $(T_0, X_0) \in W_f(k)$  and identify  $\text{Stab}(T_0) \simeq J[2]$  as in Section 2.3. To compute the image of  $\alpha$  in  $H^1(k, \text{PO}_{2n+1})$ , we choose for each  $\sigma \in \text{Gal}(k^s/k)$ , a polynomial  $h_\sigma(x) \in \mu_2(k^s[x]/f(x))$  such that  ${}^\sigma\sqrt{\alpha}/\sqrt{\alpha} = h_\sigma(\beta)$ . Then  $(h_\sigma(T_0))_\sigma$  is its image in  $H^1(k, \text{PO}_{2n+1})$ . Let  $\iota$  denote the isometry defined over  $k$  from  $(L, <, >_1)$  to  $(U_0, Q_0)$  that sends  $\cdot\beta$  to  $T_0$ . Consider the following sequence of isometries

$$(L, <, >_\alpha) \xrightarrow[k^s]{\sqrt{\alpha}} (L, <, >) \xrightarrow[k]{\iota} (U_0, Q_0) \xrightarrow[k^s]{g} (U_0, Q_0), \quad (2.9)$$

where the subscripts below the arrows indicate the fields of definition and the last map is the

standard action of some  $g \in \mathrm{O}_{2n+1}(k^s)$ .

Now  $<, >_\alpha$  is split if and only if the above composite map is defined over  $k$  for some  $g \in \mathrm{O}_{2n+1}(k^s)$  if and only if

$${}^\sigma g h_\sigma(T_0) g^{-1} = 1 \text{ for some } g \in \mathrm{O}_{2n+1}(k^s),$$

if and only if

$$h_\sigma(T_0) = {}^\sigma g^{-1} g \text{ for some } g \in \mathrm{O}_{2n+1}(k^s),$$

if and only if

$$h_\sigma(T_0) = g^{-1} {}^\sigma g \text{ for some } g \in \mathrm{PO}_{2n+1}(k^s) \text{ since } h_\sigma(T_0)^2 = 1,$$

if and only if

$$\alpha \in \ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PO}_{2n+1})). \quad \square$$

**Summary 2.14.**  $\mathrm{PO}_{2n+1}(k)$ -orbits of self-adjoint operators with characteristic polynomial  $f(x)$  are in bijection with

$$\ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PO}_{2n+1})).$$

For each  $\alpha$  in the kernel, lift it to  $L^\times$ . The quadratic space  $(L, <, >_\alpha)$  is split. Choose any isometry over  $k$  between it and the model space  $U_0$ , then the images of the multiplication by  $\beta$  operator form a complete set of representatives of the  $\mathrm{PO}_{2n+1}(k)$ .

$$\alpha = 1 \iff \textbf{distinguished orbit}$$

$$\alpha \in J(k)/2J(k) \iff \textbf{soluble orbits.}$$

## 2.5 Quadratic refinement of the Weil pairing

For any principally polarized abelian variety  $A$  and any positive integer  $n$ , there is a Weil pairing

$$A[n] \times A[n] \rightarrow \mu_n.$$

Specializing to the Jacobian  $J$  of a curve  $C$  over  $k$ , one obtains a bilinear form

$$\iota : H^1(k, J[2]) \times H^1(k, J[2]) \rightarrow H^2(k, \mu_2).$$

The goal of this subsection is to show when  $C$  is a hyperelliptic curve with a rational Weierstrass point, one can obtain a quadratic refinement of this bilinear form as follows.

Identifying  $\mathrm{PO}_{2n+1}$  with  $\mathrm{SO}_{2n+1}$ , we have the following diagram,

$$\begin{array}{ccccccc} & & & & J[2] & & \\ & & & & \downarrow & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Spin}_{2n+1} & \longrightarrow & \mathrm{SO}_{2n+1} \longrightarrow 1 \end{array}$$

where the inclusion  $J[2] \hookrightarrow \mathrm{SO}_{2n+1}$  is the identification of  $J[2]$  with the stabilizer of a fixed rational self-adjoint operator  $T$ . Taking Galois cohomology gives the following composite map of pointed sets,

$$q : H^1(k, J[2]) \rightarrow H^1(k, \mathrm{SO}_{2n+1}) \rightarrow H^2(k, \mu_2).$$

**Theorem 2.15.**  $q$  is a quadratic refinement for  $\iota$ . In other words,

$$q(v + w) - q(v) - q(w) = \iota(v, w),$$

for all  $v, w \in H^1(k, J[2])$ .

Recall that  $J[2](k^s)$  is generated by divisors of the form  $(P_i) - (\infty)$ . Denote by  $e_2$  the Weil pairing. The following formula for  $e_2$  can be checked directly from its definition.



**Lemma 2.16.**

$$e_2((P_i) - (\infty), (P_j) - (\infty)) = \begin{cases} 1 & \text{if } i = j \\ -1 & \text{if } i \neq j \end{cases}$$

In particular if we let  $P_0$  denote  $\infty$ , then

$$e_2\left(\sum_{i=0}^{2n+1} n_i(P_i), \sum_{i=0}^{2n+1} n'_i(P_i)\right) = (-1)^a$$

where  $a$  is the number of  $i$  such that  $n_i \equiv n'_i \equiv 1 \pmod{2}$ .

On the other hand, the diagram (2.9) above gives another symplectic pairing on  $J[2](k^s)$ . Namely, given any two  $[D_1], [D_2] \in J[2](k^s)$ , let  $\tilde{g}_1, \tilde{g}_2 \in \text{Spin}(k^s)$  be any lift of  $\iota([D_1]), \iota([D_2]) \in \text{SO}_{2n+1}(k^s)$ , then the element

$$([D_1], [D_2]) := \tilde{g}_1 \tilde{g}_2 \tilde{g}_1^{-1} \tilde{g}_2^{-1} \quad (2.10)$$

lies in the central  $\mu_2$  and is independent on the choices of the lifts. Notice this pairing does not depend on the rational  $T$ . If a different rational  $T'$  was used to define the inclusion from  $J[2]$  to  $\text{SO}_{2n+1}$ , one can choose some  $g \in \text{SO}_{2n+1}(k^s)$  sending one to the other. Lift it arbitrarily to  $\tilde{g} \in \text{Spin}_{2n+1}(k^s)$ , the new pairing  $([D_1], [D_2])$  would differ from the old one by conjugation by  $\tilde{g}$  which acts trivially on the central  $\mu_2$ . Denote the bilinear form from  $H^1(k, C) \times H^1(k, C)$  to  $H^2(k, A)$  induced by this pairing (2.10) by  $-\gamma_1 \cup \gamma_2$ .

**Proposition 2.17.**  $q$  is a quadratic refinement of this bilinear form.

**Proof:** Apply [14] Proposition 2.9 with  $A = \mu_2$  central in  $B = \text{Spin}_{2n+1} \times_{\text{SO}_{2n+1}} J[2]$  with abelian quotient  $C = J[2]$ .  $\square$

Therefore to prove Theorem 2.15, it suffices to show that the symplectic pairing defined in (2.10) is the same as the Weil pairing. The heuristic here is that for generic  $C$ , they both define a  $S_{2n+1}$ -invariant non-degenerate symplectic pairing

$$(\mathbb{Z}/2\mathbb{Z})^{2n+1}/(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{2n+1}/(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathbb{Z}/2\mathbb{Z}, \quad (2.11)$$

where  $S_{2n+1}$  is the symmetric group on  $2n+1$  letters. A direct combinatoric argument shows that such a pairing is unique. A rigorous argument can be made by using a family  $\mathcal{C}$  of hyperelliptic curve over a base  $V$  which we will use extensively in the next chapter. The 2-torsion  $\mathcal{J}[2]$  of its relative Picard scheme is an étale group scheme over  $S$ , and so is the Hom scheme  $\underline{\text{Hom}}_V(\mathcal{J}[2] \times \mathcal{J}[2], \mu_2)$ . The two pairings give two sections of the latter scheme over  $V$ . They coincide on the generic fiber of  $V$ , therefore they coincide throughout  $V$ .

In this section, we give a more computational proof for the equality of the two pairings as an exercise in computation in Spin. It suffices to work over the separable closure. Recalling some notations, let  $f(x)$  denote the monic polynomial of degree  $2n+1$  that defines the hyperelliptic curve  $C$ , let  $\alpha_1, \dots, \alpha_{2n+1}$  denote its roots. For each  $i$ , put  $h_i(x) = f(x)/(x - \alpha_i)$ . Let  $L$  denote the model space  $k[x]/f(x)$  of dimension  $2n+1$  with power basis  $\{1, \beta, \dots, \beta^{2n}\}$  equipped with the usual split bilinear form  $\langle, \rangle$ . Fixing an isometry over  $k$  between  $(L, \langle, \rangle)$  and the original split space  $(U, \langle, \rangle)$ , we transfer all problems over to  $L$ . Since the pairing (2.10) is independent on the choice of  $T$ , we set  $T$  to be the multiplication by  $\beta$  operator. Then  $v_i = h_i(\beta)$  is an eigenvector of  $T$  with eigenvalue  $\alpha_i$ , and they form an orthogonal basis for  $L$ . Namely,

$$\begin{aligned} \langle v_i, v_i \rangle &= h_i(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j), \\ \langle v_i, v_j \rangle &= 0, \text{ for } j \neq i \end{aligned}$$

The inclusion  $J[2] \hookrightarrow \text{SO}_{2n+1}$  is given by

$$\iota((P_i) - (\infty)) = 2 \frac{h_i(\beta)}{h_i(\alpha_i)} - 1,$$

which as we saw in the proof of Proposition 2.7 is the negative of reflection about  $v_i^\perp$ , hence has determinant 1. Note this is the negative of the formula given in Remark 1.6 due to the identification of PO with SO.

Since the characteristic of  $k$  is not 2, the Clifford algebra associated to  $(L, \langle, \rangle)$  is quotient

algebra

$$\text{Cliff}(L, <, >) = T(L)/(v \otimes w + w \otimes v - 2 < v, w >)$$

where  $T(L)$  is the tensor algebra. The group  $\text{Spin}_{2n+1}$  is the subgroup of the even part of the Clifford group  $\Gamma^0$  with Spinor norm 1. The underlying set of  $\text{Spin}_{2n+1}$  is the set of elements  $x$  in  $\text{Cliff}^0$  such that  $xvx^{-1}$  lands in  $L$  for all  $v \in L$ , and that  $x^t x = 1$  where  $t$  denotes the order reversing transpose on  $T(L)$ . To lift the image of  $(P_i) - (\infty)$ , we need to find an  $x_i \in \text{Cliff}^0$  such that

$$\begin{aligned} x_i v_i x_i^{-1} &= v_i \\ x_i v_j x_i^{-1} &= -v_j, \text{ for } j \neq i. \end{aligned}$$

A simple computation shows that  $x_i = v_1 \cdots v_{i-1} v_{i+1} \cdots v_{2n+1}$  does the job. Moreover,

$$x_i x_j = (-1)^{2n+(2n-1)(2n-1)+2n} x_j x_i = -x_j x_i.$$

Dividing  $x_i$  by a square root of its Spinor norm gives the desired lift  $\tilde{x}_i$  and

$$\begin{aligned} \tilde{x}_i \tilde{x}_i \tilde{x}_i^{-1} \tilde{x}_i^{-1} &= 1 = w((P_i) - (\infty), (P_i) - (\infty)) \\ \tilde{x}_i \tilde{x}_i \tilde{x}_j^{-1} \tilde{x}_j^{-1} &= -1 = w((P_i) - (\infty), (P_j) - (\infty)), \text{ for } j \neq i. \end{aligned}$$

Therefore, we have proved the equality of the two pairings, and thus Theorem 2.15.

## 2.6 Pencil of quadrics containing a quadric of discriminant 1

For the remainder of the chapter, we will be considering the even dimensional analogue. Let  $U$  be a  $2n + 2$  dimensional vector space over  $k$  and let  $\mathcal{L}(Q_1, Q_2)$  be a rational generic pencil of quadrics in  $\mathbb{P}^{2n+1} = \mathbb{P}(U)$  containing a rational quadric of discriminant 1. The hyperelliptic curve  $C$  associated to it will have a rational non-Weierstrass point  $P$ . Once again by moving  $P$

to  $\infty$ , we may assume  $Q_1$  has discriminant 1.

There are two rulings defined over  $k$  of  $n$ -planes contained in  $Q_1$ . These two rulings are acted on by  $\mathrm{PO}(U, Q_1)$ , each with stabilizer  $\mathrm{PSO}(U, Q_1) =: \mathrm{PSO}_{2n+2}$ . Fix  $Y_0$  to be one such ruling and let  $\infty$  be the point on the associated hyperelliptic curve corresponding to this ruling. If  $\mathbb{P}Y_1, \mathbb{P}Y_2$  are two  $n$ -planes contained in  $Q_1$ , we write  $\mathbb{P}Y_1 \sim \mathbb{P}Y_2$  if they lie in the same ruling, and we write  $\mathbb{P}Y_1 \sim Y_0$  if  $\mathbb{P}Y_1$  lies in the ruling  $Y_0$ .

Let  $b$  denote the associated bilinear form of  $Q_1$  and let  $T$  be the self-adjoint operator, with respect to  $Q_1$ , such that

$$Q_2(v) = b(v, Tv)$$

as in (1.1). The variety  $F$  of  $(n-1)$ -planes contained in the base locus fits into a disconnected algebraic group over  $k$ ,

$$G = J \dot{\cup} F \dot{\cup} \underline{\mathrm{Pic}}^1(C) \dot{\cup} F'.$$

Since  $(\infty) \in \underline{\mathrm{Pic}}^1(C)$ , we can lift  $F$  to a torsor of  $J[2]$  by taking

$$F[2]_\infty = \{\mathbb{P}X \in F \mid \mathbb{P}X +_G \mathbb{P}X = (\infty)\}.$$

**Proposition 2.18.**

$$F[2]_\infty = \{\mathbb{P}X \in F \mid \mathbb{P}X = \tau(\infty)\mathbb{P}X\} = \{\mathbb{P}X \simeq \mathbb{P}^{n-1} \mid \mathrm{Span}\{\mathbb{P}X, \mathbb{P}(TX)\} \sim Y_0\}.$$

The latter condition means  $\mathrm{Span}\{\mathbb{P}X, \mathbb{P}(TX)\}$  is an  $n$ -plane contained in  $Q_1$  in the ruling  $Y_0$ . cf. Section 1.2.2.

**Proof:** Suppose  $\mathbb{P}X \simeq \mathbb{P}^{n-1}$  with  $\mathrm{Span}\{\mathbb{P}X, \mathbb{P}(TX)\} \sim Y_0$ .

1). Since  $TX \subset X^{\perp_{Q_1}}$ , we see  $X \subset X^{\perp_{Q_2}}$  and hence  $\mathbb{P}X \in F$ .

2). Since  $\mathrm{Span}\{\mathbb{P}X, \mathbb{P}(TX)\} \supset \mathbb{P}X$  is an  $n$ -plane contained in  $Q_1$  in the same ruling as  $\mathbb{P}Y_0$ , we see  $\tau(\infty)\mathbb{P}X$  is the residual intersection of  $\mathrm{Span}\{\mathbb{P}X, \mathbb{P}(TX)\}$  with  $Q_2$ .

3).  $\text{Span}\{\mathbb{P}X, \mathbb{P}(TX)\}$  intersects  $Q_2$  tangentially at  $\mathbb{P}X$  because

$$TX \subset TX^{\perp_{Q_1}} \Rightarrow TX \subset X^{\perp_{Q_2}} \Rightarrow T_{\mathbb{P}X}Q_2 \supset \text{Span}\{\mathbb{P}X, \mathbb{P}(TX)\}.$$

Therefore  $\mathbb{P}X \in F[2]_{\infty}$ .

Conversely, suppose  $\mathbb{P}X \in F[2]_{\infty}$ . Suppose  $\text{Span}\{\mathbb{P}X, [p]\} \supset \mathbb{P}X$  is the  $n$ -plane contained in  $Q_1$  in the same ruling as  $\mathbb{P}Y_0$ , for some  $p \in U \otimes k^a$ . Since  $\tau(\infty)\mathbb{P}X = \mathbb{P}X$ , we see

$$b(x, p) = b(x, Tp) = b(p, p) = 0, \forall x \in X.$$

1). Since  $\text{Span}\{\mathbb{P}X, [p]\}$  does not lie in the base locus,  $b(p, Tp) = Q_2(p) \neq 0$ .

2). Since  $\text{Span}\{X, p\} \subset p^{\perp_{Q_1}}$ , we have  $Tp \notin \text{Span}\{X, p\}$  but  $Tp \in X^{\perp_{Q_1}}$ . Hence

$$X^{\perp_{Q_1}} = \text{Span}\{X, p, Tp\}.$$

3). Since  $TX \subset p^{\perp_{Q_1}} \cap X^{\perp_{Q_1}}$ , we have  $TX \subset \text{Span}\{X, p\}$ .

4). If  $TX \subset X$ , then  $X^{\perp_{Q_1}} = X^{\perp_{Q_2}}$  which implies that  $T_{\mathbb{P}X}(Q_1 \cap Q_2) \simeq \mathbb{P}^{n+1}$ . This contradicts

Lemma 1.15. Therefore

$$X \subsetneq TX \subset \text{Span}\{X, p\}, \quad \text{i.e.} \quad \text{Span}\{\mathbb{P}X, \mathbb{P}(TX)\} = \text{Span}\{\mathbb{P}X, [p]\} \sim Y_0. \quad \square$$

## 2.7 Orbits of an action of $\text{PSO}_{2n+2}$

Recalling some notations: let  $f(x) \in k[x]$  be any monic polynomial of degree  $2n+2$  with distinct roots splitting completely over the separable closure. We had the following  $k$ -schemes,

$$V_f = \{T : U \rightarrow U \mid T^* = T, \text{ characteristic polynomial of } T \text{ is } f\},$$

$$W_f = \{(T, X) \in V_f \times \text{Gr}(n, U) \mid \text{Span}\{X, TX\} \sim Y_0\}.$$

We want to study the  $\mathrm{PSO}_{2n+2}(k)$ -orbits of  $V_f(k)$ . We see from Proposition 1.29 that there is only one geometric orbit. Fix any  $(T_0, X_0) \in W_f(k)$ , which is nonempty by Lemma 1.30, the  $\mathrm{PSO}_{2n+2}(k)$ -orbits of  $V_f(k)$  are in bijection with

$$\ker \left( H^1(k, \mathrm{Stab}(T_0)) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}) \right). \quad (2.12)$$

By Corollary 1.33, one can identify  $\mathrm{Stab}(T)$  with  $J[2]$  and obtain a class  $c_T$  in  $H^1(k, J[2])$  by taking

$$W_T = \{X | \mathrm{Span}(X, TX) \sim Y_0\}.$$

**Lemma 2.19.** The map

$$\mathrm{PSO}_{2n+2}(k) \backslash V_f(k) \rightarrow \ker \left( H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}) \right)$$

is given by  $T \mapsto c_T$ .

**Proof:** Same Galois cohomology computation as in the proof of Lemma 2.4.  $\square$

The **distinguished** orbit corresponds to the trivial class in  $H^1(k, J[2])$ . It consists of self-adjoint operators  $T$  such that  $W_T(k) \neq \emptyset$ , namely there exists a linear  $n$ -dimensional  $k$ -subspace  $X \subset U$  such that  $\mathrm{Span}\{X, TX\}$  is an  $n+1$  dimensional isotropic subspace of  $U$  that intersects  $Y_0$  at even codimension.

The **soluble** orbits correspond to the self-adjoint operators  $T$  for which  $F_T(k) \neq \emptyset$ , namely it admits a linear  $n$ -dimensional  $k$ -subspace  $X \subset U$  such that  $\mathrm{Span}\{X, TX\} \subset X^\perp$ .

**Theorem 2.20.** The soluble orbits correspond bijectively to the image of  $J(k)/2J(k)$  in  $H^1(k, J[2])$ . In particular, the composition

$$J(k)/2J(k) \xrightarrow{\delta} H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+1})$$

is trivial.

Just as in Section 2.3, we show the soluble orbits maps into  $\delta(J(k)/2J(k))$  in this Section. Surjectivity will be proved in the next Section after a 2-descent analysis on  $J$ .

By definition,  $F_T[2]_\infty = W_T$  as  $\text{Gal}(k^s/k)$ -sets.

**Proposition 2.21.**  $F_T[2]_\infty = W_T$  as  $J[2]$ -torsors. Therefore

$$[F_T[2]_\infty] = c_T \in H^1(k, J[2]).$$

**Proof:** It suffices to show for any  $(P_1) - (P_2) \in J[2]$  with  $P_1, P_2$  any two Weierstrass points, the two actions are the same. Let  $\alpha_i$  denote the root of  $f(x)$  corresponding to  $P_i$ , and set  $h_i(x) = f(x)/(x - \alpha_i)$ . On  $W_T(k^a)$ , by Remark 1.34, the action of  $(P_1) - (P_2)$  is induced by the following map on  $U \otimes k^s$  :

$$x \mapsto x - 2 \frac{h_1(T)}{h_1(\alpha_1)} x - 2 \frac{h_2(T)}{h_2(\alpha_2)} x$$

on

For  $i = 1, 2$ , let  $w_i \in U \otimes k^s$  be an eigenvector of  $T$  with eigenvalue  $\alpha_i$ . The cone point of the singular quadric corresponding to  $P_i$  is therefore  $[w_i]$ . Let  $b$  denote the bilinear form associated to  $Q$ . Then on  $F_T(k^s)$ , similar to (2.4), the action of  $\tau(P_i)$  is induced by the following map on  $U \otimes k^a$  :

$$\text{refl}_{P_i} : x \mapsto x - 2 \frac{b(x, w_i)}{b(w_i, w_i)} w_i.$$

Composing two such reflections, we see that the action of  $\tau(P_1)\tau(P_2)$  is induced by the following map on  $U \otimes k^a$  :

$$x \mapsto x - 2 \frac{b(x, w_1)}{b(w_1, w_1)} w_1 - 2 \frac{b(x, w_2)}{b(w_2, w_2)} w_2 + \frac{4b(x, w_1)b(w_1, w_2)}{b(w_1, w_1)b(w_2, w_2)} w_2.$$

Since self-adjoint operators have pairwise orthogonal eigenspaces, the last term is 0. Also as in the proof of Proposition 2.7,

$$\frac{h_i(T)}{h_i(\alpha_i)} x = \frac{b(x, w_i)}{b(w_i, w_i)} w_i.$$

Therefore the two actions are equal. □

**Remark 2.22.** In parallel to the odd case, the equality  $F_T[2]_\infty = W_T$  as  $\text{Gal}(k^s/k)$ -sets provides a different view point on the identification of  $J[2]$  with  $\text{Stab}(T)$ , as they share a common principal homogeneous space. Proposition 2.21 implies that this new identification coincides with the formula given by Remark 1.34.

**Corollary 2.23.** The composite map

$$\text{PSO}_{2n+1}(k) \backslash V_f(k) \rightarrow H^1(k, J[2]) \rightarrow H^1(k, J)[2]$$

is given by  $T \mapsto [F_T]$ .

**Corollary 2.24.** The soluble orbits map into the image of  $J(k)/2J(k)$  in  $H^1(k, J[2])$ . The correspondence is given by  $T \mapsto c_T = \delta(\mathbb{P}X +_G \mathbb{P}X - (\infty))$  for any  $\mathbb{P}X \in F_T(k)$ .

**Proof:** Same argument as the proof of Corollary 2.10. □

## 2.8 Hyperelliptic curves with a rational non-Weierstrass point

In this section we work out some 2-descent on Jacobians of hyperelliptic curves with rational non-Weierstrass points and complete the surjectivity of Theorem 2.20.

Let  $C$  be a hyperelliptic curve of genus  $n$  with a rational non-Weierstrass point, let  $J$  denote its Jacobian. By moving the point to  $\infty$ , we can assume  $C$  is given by affine equation  $y^2 = f(x)$  where  $f(x)$  is a monic degree  $2n+2$  polynomial. Let  $\infty'$  denote its image under the hyperelliptic involution and let  $P_1, \dots, P_{2n+2}$  denote the  $2n+2$  Weierstrass points. Then

$$J[2](k^s) = \langle (P_i) + (P_j) - (\infty) - (\infty') \mid \sum_{i=1}^{2n+2} (P_i) - (n+1)((\infty) + (\infty')) = \text{div}(y) = 0 \rangle$$

is an elementary 2-group of order  $2^{2n}$ . As a group scheme over  $k$ ,

$$J[2] = (\text{Res}_{L/k} \mu_2)_{N=1} / \mu_2 \simeq (\text{Res}_{L/k} \mu_2 / \mu_2)_{N=1}$$



where  $L = k[x]/f(x) = k[\beta]$  is an étale  $k$ -algebra of dimension  $2n + 2$ . The following diagram keeps track of the  $\mu_2$ 's coming in and out of  $\text{Res}_{L/k}\mu_2$ .

$$\begin{array}{ccccc}
\mu_2 & \xrightarrow{\sim} & \mu_2 & & \\
\downarrow & & \downarrow & & \\
(\text{Res}_{L/k}\mu_2)_{N=1} & \hookrightarrow & \text{Res}_{L/k}\mu_2 & \xrightarrow{N} & \mu_2 \\
\downarrow & & \downarrow & & \downarrow \sim \\
J[2] & \hookrightarrow & \text{Res}_{L/k}\mu_2/\mu_2 & \xrightarrow{N} & \mu_2
\end{array}$$

Combining the descent sequence and the above, one obtains the following diagram.

$$\begin{array}{ccccccc}
\langle (\infty') - (\infty) \rangle & \longrightarrow & J(k)/2J(k) & \xrightarrow{\delta'} & L^\times/L^{\times 2}k^\times & \xrightarrow{N} & k^\times/k^{\times 2} \\
\downarrow \sim & & \downarrow \delta & & \downarrow & & \downarrow \sim \\
\frac{\mu_2(k)}{N(\text{Res}_{L/k}\mu_2/\mu_2(k))} & \longrightarrow & H^1(k, J[2]) & \longrightarrow & H^1(k, \text{Res}_{L/k}\mu_2/\mu_2) & \xrightarrow{N} & H^1(k, \mu_2) \\
& & \downarrow & \searrow \eta & \downarrow & & \\
& & H^1(k, J)[2] & \dashrightarrow & \ker(\text{Br}(k)[2]) & \rightarrow & \text{Br}(L)[2]
\end{array} \tag{2.13}$$

The map  $\delta'$  is defined in [15] by evaluating  $(x - \beta)$  on a given divisor class. As shown in [15], the first row is not exact: the image of  $\delta$  lands inside, generally not onto,  $(L^\times/L^{\times 2}k^\times)_{N=1}$  with kernel the class  $(\infty') - (\infty)$ . The following Lemma is immediate from the exactness of the second row and the commutativity of the top left square.

**Lemma 2.25.**  $(\infty') - (\infty) \in 2J(k)$  if and only if  $H^1(k, J[2]) \rightarrow H^1(k, \text{Res}_{L/k}\mu_2/\mu_2)$  is injective if and only if every  $\text{PO}(U, Q)(k)$ -orbit of  $V_f(k)$  stays as one  $\text{PSO}(U, Q)(k)$ -orbit.

Take any  $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$  and lift it to an element of  $L^\times$  whose norm to  $k$  is a square. Denote the lift by  $\alpha$  also and let  $\sqrt{\alpha}$  be a square root of  $\alpha$  in  $L \otimes k^s$ . Then the third vertical map

$$(L^\times/L^{\times 2}k^\times)_{N=1} \rightarrow H^1(k, \text{Res}_{L/k}\mu_2/\mu_2)$$

is given by

$$\alpha \mapsto \left( \frac{\sigma \sqrt{\alpha}}{\sqrt{\alpha}} \right)_\sigma \in H^1(\text{Gal}(k^s/k), \mu_2(L \otimes k^s)^\times / \mu_2(k^{s^\times})).$$

Consider the quadric  $Q$  on  $L$  defined by the bilinear form

$$\langle \lambda, \mu \rangle_\alpha = \text{coefficient of } \beta^{2n+1} \text{ in } \alpha \lambda \mu.$$

Since  $N_{L/k}(\alpha)$  is a square in  $k$ ,  $Q$  has discriminant 1. Choosing a different lift of  $\alpha$  does not change the  $k$ -isomorphism type of  $Q$ . Let  $T$  denote the multiplication by  $\beta$  operator.  $T$  is self-adjoint with respect to  $Q$ . Let  $Y_\alpha$  be the following  $n+1$  dimensional isotropic  $k^s$ -subspace of  $L \otimes k^s$ :

$$Y_\alpha = \text{Span}_{k^s} \left\{ \frac{1}{\sqrt{\alpha}}, \frac{\beta}{\sqrt{\alpha}}, \dots, \frac{\beta^n}{\sqrt{\alpha}} \right\}.$$

Define

$$X_\alpha = \text{Span}_{k^s} \left\{ \frac{1}{\sqrt{\alpha}}, \frac{\beta}{\sqrt{\alpha}}, \dots, \frac{\beta^{n-1}}{\sqrt{\alpha}} \right\}.$$

Since  $Q$  has discriminant 1, the ruling containing  $Y_\alpha$  is defined over  $k$  and we define  $W_T$  as in the previous section. In fact, as the following proposition shows,  $Q$  is always split when we need it to.

**Proposition 2.26.** For any  $\alpha \in (L^\times / L^{\times 2} k^\times)_{N=1}$ , there exists an  $\tilde{\alpha} \in H^1(k, J[2])$  having the same image in  $H^1(k, \text{Res}_{L/k} \mu_2 / \mu_2)$  as  $\alpha$ .

$$\langle, \rangle_\alpha \text{ is split} \iff \tilde{\alpha} \in \ker(H^1(k, J[2]) \rightarrow H^1(k, \text{PSO}_{2n+2})).$$

**Proof:** The first claim follows because the image of  $\alpha$  in  $H^1(k, \text{Res}_{L/k} \mu_2 / \mu_2)$  has norm 1. For the second statement, one can follow the proof of Proposition 2.13 to show that  $\langle, \rangle_\alpha$  is split if and only if

$$\tilde{\alpha} \in \ker(H^1(k, J[2]) \rightarrow H^1(k, \text{PO}_{2n+2})).$$

On the other hand,

$$\ker(H^1(k, \mathrm{PSO}_{2n+2}) \rightarrow H^1(k, \mathrm{PO}_{2n+2})) \simeq \mathrm{coker}(\mathrm{PO}_{2n+2}(k) \rightarrow \mu_2(k)) = 1,$$

since reflection  $x \mapsto x - 2 \frac{\langle x, v \rangle_\alpha}{\langle v, v \rangle_\alpha} v$  about  $v^\perp$  for any  $k$ -rational vector  $v$  is an element of  $O_{2n+2}(k)$  of determinant -1.  $\square$

On  $\mathbb{P}L$ , there is a rational generic pencil of quadrics spanned by  $Q, Q_T$  given by the following formula in terms of quadratic forms:

$$\begin{aligned} Q(v) &= \langle v, v \rangle_\alpha \\ Q_T(v) &= \langle v, \beta v \rangle_\alpha. \end{aligned}$$

Since  $Q$  has discriminant 1 and  $T$  has characteristic polynomial  $f(x)$ , the hyperelliptic curve associated to this pencil is  $C$ . Suppose  $\infty$  corresponds to the ruling on  $Q$  containing  $\mathbb{P}Y_0$ . Taking the variety  $F_T$  of  $(n-1)$ -planes in the base locus of the pencil in  $\mathbb{P}(L)$  gives a torsor of  $J$  of order dividing 2. As before, we define

$$F_T[2]_\infty = \{\mathbb{P}X \in F \mid \mathbb{P}X +_G \mathbb{P}X = (\infty)\}.$$

**Proposition 2.27.**  $[F_T[2]_\infty] \in H^1(k, J[2])$  maps to the same class in  $H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2)$  as  $\alpha$ . In particular, every class in  $\ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}))$  arises from pencils of quadrics.

**Proof:** By Proposition 2.21,  $F_T[2]_\infty = W_T$  as  $J[2]$ -torsors. The first statement follows as

$$\mathrm{Span}\{X_\alpha, TX_\alpha\} = Y_\alpha \sim Y_0 \Rightarrow X_\alpha \in W_T(k^s),$$

and

$$X_\alpha^\sigma = \frac{\sqrt{\alpha}^\sigma}{\sqrt{\alpha}} X_\alpha$$

for all  $\sigma \in \mathrm{Gal}(k^s/k)$ .

For the second statement, suppose  $c \in \ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}))$  is killed by  $\eta$ . Then its image  $c'$  in  $H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2)$  comes from some  $\alpha \in L^\times/L^{\times 2}k^\times$ . Furthermore,  $N_{L/k}(\alpha) = N(c') = 1$ . Hence  $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$  gives rise to a pencil of quadrics. Denote by  $F_T[2]_{\infty'}$  the lift of  $F$  by  $(\infty')$ . Then

$$[F_T[2]_{\infty'}] = [F_T[2]_{\infty}] + \delta((\infty') - (\infty)) \mapsto c'.$$

One of  $[F_T[2]_{\infty}], [F_T[2]_{\infty'}]$  recovers  $c$ . The proof is complete after applying the following Proposition.  $\square$

**Proposition 2.28.**

$$\eta(\ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}))) = 1.$$

**Proof:** From the two diagrams,

$$\begin{array}{ccccccc} \mathrm{Stab}_{\mathrm{PSO}}(T) & \longrightarrow & \mathrm{Stab}_{\mathrm{PO}}(T) & & 1 & \longrightarrow & \mu_2 \longrightarrow \mathrm{Stab}_O(T) \longrightarrow \mathrm{Stab}_{\mathrm{PO}}(T) \longrightarrow 1 \\ \downarrow & & \downarrow & & \downarrow = & & \downarrow \\ \mathrm{PSO}(U, Q) & \longrightarrow & \mathrm{PO}(U, Q) & & 1 & \longrightarrow & \mu_2 \longrightarrow O(U, Q) \longrightarrow \mathrm{PO}(U, Q) \longrightarrow 1, \end{array}$$

one gets a commuting diagram, of non-exact rows,

$$\begin{array}{ccccc} H^1(k, \mathrm{Stab}_{\mathrm{PSO}}(T)) & \longrightarrow & H^1(k, \mathrm{Stab}_{\mathrm{PO}}(T)) & \longrightarrow & H^2(k, \mu_2) \\ \downarrow & \searrow \eta & \downarrow & & \downarrow = \\ H^1(k, \mathrm{PSO}(U, Q)) & \longrightarrow & H^1(k, \mathrm{PO}(U, Q)) & \longrightarrow & H^2(k, \mu_2). \end{array}$$

The result is now immediate.  $\square$

The upshot of this Proposition is that even though we don't understand all of  $H^1(k, J[2])$ , we know enough to study  $\mathrm{PSO}_{2n+2}(k)$ -orbits. Consider the soluble ones first. Suppose  $\alpha = \delta'([D])$  for some  $[D] \in J(k)/2J(k)$ . By Proposition 2.27, we see that  $F_T(k)$  is non-empty and that for

any  $\mathbb{P}X \in F_T(k)$ ,

$$\mathbb{P}X +_G \mathbb{P}X - (\infty_D) = [D] \pmod{2J(k)}.$$

If  $\mathbb{P}X \in F_T[2]_\infty$ , then  $\text{Span}\{X, TX\}$  is a  $k$ -rational maximal isotropic subspace of  $(L, <, >_\alpha)$ . If  $\mathbb{P}X \notin F_T[2]_\infty$ , then  $\text{Span}\{X, \tau(\infty)X\}$  is a  $k$ -rational maximal isotropic subspace of  $(L, <, >_\alpha)$ . In either cases,  $(L, <, >_\alpha)$  is split and Proposition 2.27 applies. Since both  $F_T[2]_\infty$  and  $F_T[2]_{\infty'}$  map to the image of  $\alpha$  in  $H^1(k, \text{Res}_{L/k}\mu_2/\mu_2)$ , one of them equals to  $\delta([D])$ . Let  $(\infty_D)$  be either  $\infty$  or  $\infty'$  such that

$$F_T[2]_{\infty_D} = \delta([D]).$$

$(\infty_D)$  is well defined up to  $2J(k)$ . Note  $[F_T]$  is the image of  $[F_T[2]_{\infty_D}]$  in  $H^1(k, J)[2]$ , and is therefore trivial.

Since  $(L, <, >_\alpha)$  is split, one can choose an isometry over  $k$  between  $(L, <, >_\alpha)$  and  $(U, Q)$  sending the ruling corresponding to  $\infty_D$  to the fixed ruling on  $U$ . Let  $T_1 \in V_f(k)$  denote the image of  $T$ . Any two such isometries differ by some  $\text{SO}(U, Q)(k)$ . Hence we get a well-defined  $\text{SO}(U, Q)(k)/(\pm 1)$ -orbit. As the following lemma shows, different  $[D]$  gives rise to different  $\text{PSO}_{2n+2}(k)$ -orbit.

**Lemma 2.29.**  $\delta([D]) = c_{T_1}$ .

**Proof:** Let  $T_0$  denote the image of  $T$  under an isometry over  $k$  between  $(L, <, >_\alpha)$  and  $(U, Q)$  that sends the ruling corresponding to  $\infty$  to the fixed ruling on  $U$ . Then

$$\delta([D] + (\infty_D) - (\infty)) = [F_T[2]_\infty] = c_{T_0}.$$

If  $\infty_D = \infty \pmod{2J(k)}$ , then we are done. Otherwise, by Lemma 2.25,  $T_0$  and  $T_1$  lie in the same  $\text{PO}(U, Q)(k)$ -orbit, but distinct  $\text{PSO}(U, Q)(k)$ -orbits. Hence  $c_{T_1} - c_{T_0}$  is the nontrivial element in

$$\ker(H^1(k, J[2]) \rightarrow H^1(k, \text{Res}_{L/k}\mu_2/\mu_2))$$

which is precisely  $\delta((\infty_D) - (\infty))$ . □

**Remark 2.30.** The difference between  $\mathrm{SO}(U, Q)(k)/(\pm 1)$  and  $\mathrm{PSO}_{2n+2}(k)$  is in fact  $k^\times/k^{\times 2}$ .

Consider the following diagram,

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & Z & \longrightarrow & \mu_2 \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Spin}_{2n+2} & \longrightarrow & \mathrm{SO}_{2n+2} \longrightarrow 1 \\
& & & & & & \downarrow \\
& & & & & & \mathrm{PSO}_{2n+2}
\end{array} ,$$

where  $Z = \mu_4$  or  $\mu_2 \times \mu_2$  is the center of  $\mathrm{Spin}_{2n+2}$ . Taking cohomology, we get

$$\begin{aligned}
\mathrm{coker}(\mathrm{SO}_{2n+2}(k) \rightarrow \mathrm{PSO}_{2n+2}(k)) &\simeq \ker(H^1(k, \mu_2) \rightarrow H^1(k, \mathrm{SO}_{2n+2})) \\
&\simeq \ker(H^1(k, \mu_2) \rightarrow H^2(k, \mu_2)) \\
&\simeq \mathrm{coker}(H^1(k, \mu_2) \rightarrow H^1(k, Z)) \\
&\simeq k^\times/k^{\times 2}.
\end{aligned}$$

We have now established the surjectivity in Theorem 2.20, restated below. It looks, as expected, exactly the same as Theorem 2.12.

**Theorem 2.31.** There is a bijection between  $J(k)/2J(k)$  and soluble orbits of self-adjoint operators with characteristic polynomial  $f(x)$ .

Moving on to all the other  $\mathrm{PSO}_{2n+2}(k)$ -orbits. By Proposition 2.28, for every class in

$$\tilde{\alpha} \in \ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2})),$$

there exists an  $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$  such that either  $F_T[2]_\infty$  or  $F_T[2]_{\infty'}$  recovers  $\tilde{\alpha}$ . By Proposition 2.26,  $<, >_\alpha$  is split and hence one can identify  $L$  with  $U$  matching the rulings as above. The image of  $T$  under the identification gives us a  $\mathrm{PSO}_{2n+2}(k)$ -orbit whose class in  $H^1(k, J[2])$  is  $\tilde{\alpha}$ .

**Summary 2.32.**  $\mathrm{PSO}_{2n+2}(k)$ -orbits of self-adjoint operators with characteristic polynomial  $f(x)$  are in bijection with

$$\ker(H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2})).$$

For each  $\tilde{\alpha}$  in the kernel, there exists  $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$  and a choice of a point  $\infty_{\tilde{\alpha}}$  above  $\infty_{\mathbb{P}^1}$  such that  $\tilde{\alpha} = [F_T[2]_{\infty_{\tilde{\alpha}}}]$ . The quadratic space  $(L, <, >_\alpha)$  is split. Choose any isometry over  $k$  between it and the model space  $U$  sending the ruling corresponding to  $\infty_{\tilde{\alpha}}$  to the fixed ruling on  $U$  containing  $Y_0$ , then the images of the multiplication by  $\beta$  operator form a complete set of representatives of the  $\mathrm{PSO}_{2n+2}(k)$ .

$$\tilde{\alpha} = 1 \iff \textbf{distinguished orbit}$$

$$\tilde{\alpha} \in J(k)/2J(k) \iff \textbf{soluble orbits}.$$

### The cohomological map $\eta$

Recall the short exact sequence

$$1 \rightarrow \mu_2 \rightarrow (\mathrm{Res}_{L/k}\mu_2)_{N=1} \rightarrow J[2] \rightarrow 1,$$

which gives rise to a long exact sequence in cohomology,

$$H^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1}) \rightarrow H^1(k, J[2]) \xrightarrow{\eta} H^2(k, \mu_2).$$

This map  $\eta$  coincides with the  $\eta$  defined in (2.13).

Let  $W[2]$  denote the class in  $H^1(k, J[2])$  corresponding to the torsor

$$W[2] = \{D \in \underline{\mathrm{Pic}}^1(C) \mid 2D = D_0\}.$$

Then  $W[2]$  lifts the class  $[\underline{\mathrm{Pic}}^1(C)] \in H^1(k, J)[2]$ , which in the current case is trivial since  $C$  has a rational point.

**Theorem 2.33.**  $\eta$  is given by cup product with  $W[2]$ .

**Proof:** This is proved in [15] Proposition 10.3 in a more general setting. The proof given here is a cleaner version of the same cocycle computation thanks to the explicit formula of the Weil pairing. Let  $P$  denote a fixed Weierstrass point. Then as a class in  $H^1(k, J[2])$ ,  $W[2]_\sigma = \sigma(P) - P$ , for any  $\sigma \in \text{Gal}(k^s/k)$ . Let  $c = (c_\sigma)_\sigma$  be any class in  $H^1(k, J[2])$ , then by definition of cup product,

$$(W[2] \cup c)_{\sigma, \tau} = e_2(\sigma(P) - P, \sigma(c_\tau)).$$

The identification  $J[2] \simeq (\text{Res}_{L/k}\mu_2)_{N=1}/\mu_2$  allows us to view each  $c_\sigma$  as a  $(2n+2)$ -tuple of  $\pm 1$  indexed by the Weierstrass points, modulo the diagonal  $\mu_2$ . Let  $\tilde{c} = (\tilde{c}_\sigma)_\sigma$  be a lift of  $c$  to a 1-cochain with value in  $(\text{Res}_{L/k}\mu_2)_{N=1}$ . If  $P'$  is any Weierstrass point, write  $\tilde{c}_\sigma(P')$  for the entry corresponding to  $P'$ . Then from the explicit formula for the Weil pairing in Lemma 2.39, we see that,

$$(W[2] \cup c)_{\sigma, \tau} = \tilde{c}_\tau(P) \cdot \tilde{c}_\tau(\sigma^{-1}(P)).$$

Let  $(a_\sigma)_\sigma$  be the 1-cochain  $a_\sigma = \tilde{c}_\sigma(P)$  with value in  $\mu_2$ . Then its coboundary is

$$(\delta a)_{\sigma, \tau} = \tilde{c}_\sigma(P) \cdot \tilde{c}_\tau(P) \cdot \tilde{c}_{\sigma\tau}(P).$$

Finally,  $\eta(c)$  as a 2-cochain lies in the diagonal  $\mu_2$  in  $(\text{Res}_{L/k}\mu_2)_{N=1}$ , and hence,

$$\begin{aligned} (\eta(c))_{\sigma, \tau} &= \tilde{c}_\sigma(P) \cdot \sigma(\tilde{c}_\tau)(P) \cdot \tilde{c}_{\sigma\tau}(P) \\ &= \tilde{c}_\sigma(P) \cdot \tilde{c}_\tau(\sigma^{-1}(P)) \cdot \tilde{c}_{\sigma\tau}(P) \\ &= (W[2] \cup c)_{\sigma, \tau} \cdot (\delta a)_{\sigma, \tau} \end{aligned}$$

Therefore as elements of  $H^2(k, \mu_2)$ ,

$$W[2] \cup c = \eta(c). \quad \square$$



**Corollary 2.34.** The map  $\eta$  is trivial if and only if  $(\infty') - (\infty) \in 2J(k)$ .

**Proof:** This follows immediately from Theorem 2.33 after noticing that the class of  $W[2]$  in  $H^1(k, J[2])$  is the Kummer image of  $(\infty') - (\infty) \in J(k)$ .  $\square$

The following result in [15] gives a criterion for when  $(\infty') - (\infty)$  is divisible by 2.

**Proposition 2.35.**  $k$  is any field. Then  $(\infty') - (\infty) \in 2J(k)$  if and only if

1.  $f(x)$  has a factor of odd degree in  $k[x]$  or
2.  $n$  is even and  $f(x)$  factors over some quadratic extension  $K$  of  $k$  as  $h(x)\bar{h}(x)$  where  $h(x) \in K[x]$  and  $\bar{h}(x)$  is the  $\text{Gal}(K/k)$ -conjugate of  $h(x)$ .

Condition (2) is equivalent to saying  $n$  is even, and every  $k_i/k$  contains the same quadratic extension of  $k$ .

This line of thought gives an amusing proof for:

**Corollary 2.36.** Any field extension of even degree over a  $p$ -adic local field with  $p \neq 2$  admits a quadratic subextension.

**Proof:** Let  $L = k[x]/f(x)$  be this field extension with  $f$  monic and irreducible and take the hyperelliptic curve  $C$  with affine equation  $y^2 = f(x)$ . If  $L$  doesn't contain a quadratic subextension of  $k$ , then  $(\infty') - (\infty)$  is a nontrivial element of  $J(k)/2J(k)$ , which when  $p \neq 2$  is isomorphic to  $J[2](k)$ . Taking the cohomology of the short exact sequence

$$1 \rightarrow J[2] \rightarrow \text{Res}_{L/k}\mu_2/\mu_2 \xrightarrow{N} \mu_2 \rightarrow 1$$

gives an injection  $J[2](k) \hookrightarrow \text{Res}_{L/k}\mu_2/\mu_2(k)$ . Therefore  $\text{Res}_{L/k}\mu_2/\mu_2(k)$  is nontrivial. One also has the exact sequence

$$1 \rightarrow \mu_2(k) \rightarrow \text{Res}_{L/k}\mu_2(k) \rightarrow \text{Res}_{L/k}\mu_2/\mu_2(k) \rightarrow k^\times/k^{\times 2} \xrightarrow{\delta} L^\times/L^{\times 2}.$$

The fact that  $L$  doesn't contain a quadratic extension of  $k$  implies that  $\delta$  is injective. Since  $\text{Res}_{L/k}\mu_2(k) = \mu_2(L)$  is isomorphic to  $\mu_2(k)$ , this sequence implies that  $\text{Res}_{L/k}\mu_2/\mu_2(k)$  is trivial. Contradiction.  $\square$

**Remark 2.37.** There is, as one would expect, a direct proof of Corollary 2.36. Indeed, the statement is immediate if the maximal unramified subextension  $k'/k$  is even. Otherwise, let  $\pi_L, \pi_k$  denote the corresponding uniformizers and denote by  $e$  the ramification degree. One can write  $\pi_L^e = \pi_k u_L$  for some unit  $u_L$  in  $\mathcal{O}_L$ . Since  $L/k'$  is totally ramified,  $\mathcal{O}_L/\pi_L \simeq \mathcal{O}_{k'}/\pi_k$  and since every element in  $1 + \pi_L \mathcal{O}_L$  is a square, we can write  $u_L$  as the product of a unit  $u_{k'}$  in  $\mathcal{O}_{k'}$  with a square in  $L$ . We can also write  $u_{k'}$  as the product of a unit  $u_k$  in  $\mathcal{O}_k$  with a square in  $k'$ . This follows from the fact that for an odd extension of finite fields  $k_2/k_1$ , the map  $k_1^\times/k_1^{\times 2} \rightarrow k_2^\times/k_2^{\times 2}$  is an isomorphism. Since  $e$  is assumed to be even, we have written  $\pi_k u_k$  as a square in  $L$  and the result follows.

## 2.9 Quadratic refinement of the Weil pairing, even case

Similar to the case with a rational Weierstrass point, we also have a quadratic refinement for the Weil pairing on the 2-torsion of the Jacobian  $J$  of a hyperelliptic curve  $C$  with a rational non-Weierstrass point. Consider the following diagram.

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \mu_2 & \longrightarrow & \text{Spin}_{2n+2} & \longrightarrow & \text{SO}_{2n+2} \longrightarrow 1 \\
 & & \downarrow & & \downarrow \text{id} & & \downarrow \\
 1 & \longrightarrow & Z & \longrightarrow & \text{Spin}_{2n+2} & \longrightarrow & \text{PSO}_{2n+2} \longrightarrow 1
 \end{array}$$

$J[2]$   
 $\swarrow$  (dotted arrow from  $J[2]$  to  $\text{SO}_{2n+2}$ )  
 $\searrow$  (solid arrow from  $J[2]$  to  $\text{PSO}_{2n+2}$ )

where the inclusion  $J[2] \hookrightarrow \text{PSO}_{2n+2}$  is the identification of  $J[2]$  with the stabilizer of a fixed rational self-adjoint operator  $T$ , the center  $Z$  is either  $\mu_4$  when  $n$  is odd or  $\mu_2 \times \mu_2$  with  $n$  is even. The dotted arrow from  $J[2]$  to  $\text{SO}_{2n+2}$  means that if  $[D_1], [D_2]$  are two distinct element in  $J[2]$ , their images in  $\text{PSO}_{2n+2}$  lifts to commuting elements in  $\text{SO}_{2n+2}$ , as one can see from

the explicit formulas described in Remark 1.34. Taking Galois cohomology gives the following composite map of pointed sets,

$$q : H^1(k, J[2]) \rightarrow H^1(k, \mathrm{PSO}_{2n+2}) \rightarrow H^2(k, Z).$$

Let  $\iota$  denote the composition of the Weil pairing with the inclusion of  $\mu_2 \hookrightarrow Z$  in the first column of the above diagram. Also denote by  $\iota$  the induced map on cohomology,

$$\iota : H^1(k, J[2]) \times H^1(k, J[2]) \rightarrow H^2(k, \mu_2) \rightarrow H^2(k, Z).$$

**Theorem 2.38.**  $q$  is a quadratic refinement for  $\iota$ . In other words,

$$q(v + w) - q(v) - q(w) = \iota(v, w),$$

for all  $v, w \in H^1(k, J[2])$ .

Recall that  $J[2](k^s)$  is generated by divisors of the form  $(P_i) + (P_j) - (\infty) - (\infty')$ . As in the odd case, one has the following formula for the Weil pairing  $e_2$  which one can check directly from its definition.

**Lemma 2.39.**

$$e_2 \left( \sum n_i(P_i) - \frac{(\sum n_i)}{2}((\infty) + (\infty')), \sum n'_i(P_i) - \frac{(\sum n'_i)}{2}((\infty) + (\infty')) \right) = (-1)^a$$

where  $a$  is the number of  $i$  such that  $n_i \equiv n'_i \equiv 1 \pmod{2}$ .

We also have the commutator pairing  $(, )$  obtained by lifting to Spin then taking the commutator. Due to the dotted arrow from  $J[2]$  to  $\mathrm{SO}_{2n+2}$ , the commutator pairing in fact takes value in  $\mu_2 \hookrightarrow Z$ . For generic curve  $C$ , both the Weil pairing and the commutator pairing define a  $S_{2n+2}$ -invariant non-degenerate symplectic pairing on  $(\mathbb{Z}/2\mathbb{Z})_{N=1}^{2n+2}/(\mathbb{Z}/2\mathbb{Z})$ . A direct combinatoric argument shows the uniqueness of such a pairing, and the same spreading out argument as in

Section 2.5 can be used to prove equality for all curves  $C$ .

The direct approach of expliciting writing down a lift in  $\text{Spin}$  also works in this case. For completeness, we write down the lift of  $(P_i) + (P_j) - (\infty) - (\infty')$ . Pass to the separable closure, let  $f(x)$  be the defining monic polynomial of degree  $2n+2$  of  $C$ . Let  $L = k[x]/f(x)$  be the model space with power basis generated by  $\beta$  and split form  $<, >$ . Let  $\alpha_i$  denote the roots of  $f$  and set  $h_i(x) = f(x)/(x - \alpha_i)$ . Let  $T$  denote the multiplication by  $\beta$  operator, then its eigenvectors are  $v_i = h_i(\beta)$  with eigenvalues  $\alpha_i$ . The element  $x_{ij} = v_i v_j$  lies in the even part of the Clifford group, its image in  $\text{PSO}_{2n+2}$  is the image of  $(P_i) + (P_j) - (\infty) - (\infty')$ . Dividing it by a square root of its Spinor norm gives the lift in  $\text{Spin}_{2n+2}$ . Computing the commutator of any two elements of this form verifies the equality of the Weil pairing and the commutator pairing.

## 2.10 Explicit computation

### 2.10.1 Case of a rational Weierstrass point

Recalling notations, let  $L = k(\beta) = k[x]/f(x)$  be spanned as a  $k$ -vector space by  $\{1, \beta, \dots, \beta^{2n}\}$  where  $f(x) = x^{2n+1} + c_{2n}x^{2n} + \dots + c_0$  is the minimal polynomial of  $\beta$ . Suppose  $f(x)$  splits over  $k^s$  with no repeated factors. Take  $\alpha \in (L^\times/L^{\times 2})_{N=1}$ , let  $<, >_\alpha$  denote the pairing on  $L$  defined in Section 2.4. We have the following two quadratic forms on  $L \oplus k$ ,

$$\begin{aligned} Q_1(v, w) &= <v, v>_\alpha = \text{Tr}(\alpha v^2/f'(\beta)) \\ Q_2(v, w) &= <v, \beta v>_\alpha + w^2 = \text{Tr}(\alpha v^2/f'(\beta)) + w^2. \end{aligned}$$

Denote its associated hyperelliptic curve by  $C$ . We have seen the variety

$$F = \{\mathbb{P}X \simeq \mathbb{P}^{n-1} | X \subset X^{\perp_{Q_1}}, X \subset X^{\perp_{Q_2}}\}$$

fits into a disconnected commutative algebrac group

$$G = J \dot{\cup} F \dot{\cup} \underline{\text{Pic}}^1(C) \dot{\cup} F'.$$

When  $\alpha$  is the image of the Kummer map of some  $[D] \in J(k)/2J(k)$ ,  $F$  has a  $k$ -rational element. The goal of this subsection is to explicitly construct a  $\mathbb{P}X$  in  $F(k)$  and show  $\mathbb{P}X +_G \mathbb{P}X - (\infty) = [D]$  directly.

Let us start with the three simplest case before we show it in the general case. The dimensions used in this subsection are linear, not projective.

**Example 2.40.** Suppose  $[D] = (P) - (\infty)$  where  $P \in C(k)$ , denote by  $x_0$  the  $x$ -coordinate of  $P$ . The two quadratic forms take the form,

$$\begin{aligned} Q_D(v, w) &= \text{Tr}((x_0 - \beta)v^2 / f'(\beta)) \\ Q'_D(v, w) &= \text{Tr}((x_0 - \beta)\beta v^2 / f'(\beta)) + w^2. \end{aligned}$$

The  $n$ -plane

$$X = \text{Span}\{(1, 0), \dots, (\beta^{n-2}, 0), (\beta^{n-1}, 1)\}$$

is  $k$ -rational and is isotropic with respect to both quadratic forms. Consider now the  $(n+1)$ -plane  $Y = \text{Span}\{X, (g(\beta), 0)\}$  where  $g$  is given by

$$\begin{aligned} g(t) &= \frac{f(t) - f(x_0)}{t - x_0} \\ &= t^{2n} + (c_{2n} + x_0)t^{2n-1} + \dots. \end{aligned}$$

Note  $g$  was chosen such that

$$(x_0 - \beta)g(\beta) = f(x_0) - f(\beta) = f(x_0).$$

It is now easy to see that  $\mathbb{P}Y$  intersect the base locus tangentially at  $\mathbb{P}X$  as  $(x_0 - \beta)\beta^i g(\beta)$  has no  $\beta^{2n}$  term for  $i = 0, \dots, n$ .

**Remark 2.41.** Here we only need  $(x_0 - \beta)g(\beta)$  to be a polynomial in  $\beta$  of degree at most  $n - 1$ , however one observes that different choices of this polynomial only affects the terms in  $g(t)$  of

degree  $n - 2$  or less, and hence no change to  $Y$ .

Now to see which quadric  $\mathbb{P}Y$  lies on, one computes:

$$\begin{aligned}
Q_D((g(\beta), 0)) &= \text{Tr}((x_0 - \beta)g(\beta)^2/f'(\beta)) \\
&= \text{Tr}(f(x_0)g(\beta)/f'(\beta)) \\
&= f(x_0) \\
Q'_D((g(\beta), 0)) &= \text{Tr}((x_0 - \beta)\beta g(\beta)^2/f'(\beta)) \\
&= \text{Tr}(f(x_0)\beta g(\beta)/f'(\beta)) \\
&= f(x_0)\text{Tr}(\beta^{2n+1} + (c_{2n} + x_0)\beta^{2n} + \cdots / f'(\beta)) \\
&= x_0 f(x_0),
\end{aligned}$$

from which one concludes that  $\mathbb{P}Y$  lies on the quadric  $x_0 Q_D - Q'_D$ . Therefore  $\mathbb{P}X +_G \mathbb{P}X = (P)$  or  $(\bar{P})$  in  $G$ , where  $\bar{\{\}}$  denotes the hyperelliptic involution. Note  $(P) - (\infty) = (\bar{P}) - (\infty) = [D]$  in  $J(k)/2J(k)$ . Therefore this confirms the claim for  $[D] = (P) - (\infty)$ .

**Example 2.42.** Suppose now  $[D] = (P) + (Q) - 2(\infty)$  with  $P = (x_1, y_1), Q = (x_2, y_2)$  in  $C(k)$ . The quadratic forms now look like:

$$\begin{aligned}
Q_D(v, w) &= \text{Tr}((x_1 - \beta)(x_2 - \beta)v^2/f'(\beta)) \\
Q'_D(v, w) &= \text{Tr}((x_1 - \beta)(x_2 - \beta)\beta v^2/f'(\beta)) + w^2.
\end{aligned}$$

Denote by  $h_1(t), h_2(t)$  the polynomials constructed above such that,

$$\begin{aligned}
(x_1 - \beta)h_1(\beta) &= f(x_1) = y_1^2 \\
(x_2 - \beta)h_2(\beta) &= f(x_2) = y_2^2.
\end{aligned}$$

The  $n$ -plane

$$X = \text{Span}\{(1, 0), \dots, (\beta^{n-2}, 0), (-y_2 h_1(\beta) + y_1 h_2(\beta), y_1 y_2 (x_1 - x_2))\}$$

is a  $k$ -rational common isotropic space for  $Q_D, Q'_D$ . To verify the claim, we need to show that

$$(P) - \mathbb{P}X = (\infty) - ((Q) - \mathbb{P}X). \quad (2.14)$$

As before, we don't need to worry about which ruling the  $(n+1)$ -plane actually lies on, as long as there is one ruling that works.

The point  $P$  corresponds to the quadric

$$x_1 Q_D - Q'_D(v, w) = \text{Tr}((x_1 - \beta)^2 (x_2 - \beta) v^2 / f'(\beta)) - w^2.$$

The  $(n+1)$ -plane

$$Y_P = \text{Span}\{X, (h_1(\beta), 0)\}$$

is isotropic with respect to it.  $\mathbb{P}Y_P$  intersect the base locus at  $\mathbb{P}X$  and

$$(P) - \mathbb{P}X = \mathbb{P}\text{Span}\{(1, 0), \dots, (\beta^{n-2}, 0), (y_2 h_1(\beta) + y_1 h_2(\beta), y_1 y_2 (x_1 - x_2))\}.$$

Likewise,

$$Y_Q = \text{Span}\{X, (h_2(\beta), 0)\},$$

$$(Q) - \mathbb{P}X = \mathbb{P}\text{Span}\{(1, 0), \dots, (\beta^{n-2}, 0), (-y_2 h_1(\beta) - y_1 h_2(\beta), y_1 y_2 (x_1 - x_2))\}.$$

This verifies (2.14) as the involution on  $A$  given by  $\infty$  is induced from the map on  $V_{2n+1} \oplus k$  sending  $(v, w)$  to  $(v, -w)$ .

**Example 2.43.** Suppose once again  $[D] = (P) + (Q) - 2(\infty)$  where  $P, Q$  are defined over a quadratic extension of  $k$  and  $Q = P^\sigma$  where  $\sigma$  is the unique nontrivial Galois automorphism.

Note the  $n$ -plane

$$X = \text{Span}\{(1, 0), \dots, (\beta^{n-2}, 0), (-y_2 h_1(\beta) + y_1 h_2(\beta), y_1 y_2 (x_1 - x_2))\}$$

is  $k$ -rational as  $\sigma$  sends the last basis vector of  $X$  to its negative and hence no effect on  $X$ . However, one now needs to be careful about rulings. In the notation of the above example, if the  $n + 1$  plane  $Y_P$  corresponds to the ruling for  $P$ , then we have also chosen the correct  $n + 1$  plane for  $Q = {}^\sigma P$  since  ${}^\sigma Y_P = Y_Q$ . If  $Y_P$  corresponds to the ruling for  $\overline{P}$ , then we have shown

$$\mathbb{P}X +_G \mathbb{P}X = (\overline{P}) + (\overline{Q}) - (\infty) = [D] \quad \text{in } J(k)/2J(k).$$

**General Case.** Write  $[D] = (P_1) + \dots + (P_m) - m(\infty) \in J(k)$  with  $m$  minimal and  $P_i = (x_i, y_i)$ . The quadratic forms look like,

$$\begin{aligned} Q_D(v, w) &= \text{Tr}((x_1 - \beta)(x_2 - \beta) \cdots (x_m - \beta)v^2 / f'(\beta)) \\ Q'_D(v, w) &= \text{Tr}((x_1 - \beta)(x_2 - \beta) \cdots (x_m - \beta)\beta v^2 / f'(\beta)) + w^2. \end{aligned}$$

As above, let  $h_i(t)$  be the polynomial such that  $(x_i - \beta)h_i(\beta) = f(x_i) = y_i^2$ . We now construct an analogue of the polynomial  $g(t)$  as follows. Write

$$U = \prod_{1 \leq i < j \leq m} (x_i - x_j)$$

for the Vandermonde polynomial, and for each  $i = 1, \dots, m$ ,

$$q_i = \prod_{1 \leq j \leq m, j \neq i} (x_j - x_i), \quad a_i = U/q_i.$$

**Lemma 2.44.** 1.  $Q_D(h_i(\beta), 0) = q_i f(x_i), \quad Q'_D(h_i(\beta), 0) = x_i q_i f(x_i).$



$$2. \sum_{i=1}^m x_i^l a_i = 0, \text{ for } l = 0, \dots, m-2.$$

$$3. \sum_{i=1}^m x_i^{m-1} a_i = (-1)^{m-1} U.$$

4. Define

$$g_j(t) = \sum_{i=1}^m x_i^j a_i \frac{y_1 \cdots y_m}{y_i} h_i(t).$$

When  $m = 2m'$  is even, the  $(m' + 1)$ -plane

$$Z_0 = \text{Span}\{(g_0(\beta), 0), \dots, (g_{m'-2}(\beta), 0), (g_{m'-1}(\beta), y_1 \cdots y_m U)\}$$

is  $k$ -rational and isotropic with respect to both quadratic forms.

**Proof.** (1) follows from the definition of  $h_i$ . Switching  $x_i$  with  $x_j$  sends  $q_i, q_j, q_k$  to  $q_j, q_i, q_k$  respectively for  $k \neq i, j$ . As  $U$  is alternating in the  $x_i$ 's, so is  $\sum_{i=1}^m x_i^l a_i$ , for any  $l$ . Since any alternating form is a polynomial multiple of  $U$ , comparing degrees and leading terms gives (2), (3). (4) follows as

$$\begin{aligned} Q_D(g_j(\beta), *) &= U \sum_{i=1}^n x_i^{2j} a_i \cdot f(x_1) \cdots f(x_n) = 0, \quad j = 0, \dots, m' - 1 \\ Q'_D(g_j(\beta), 0) &= U \sum_{i=1}^n x_i^{2j+1} a_i \cdot f(x_1) \cdots f(x_n) = 0, \quad j = 0, \dots, m' - 2 \\ Q'_D(g_{m'-1}(\beta), y_1 \cdots y_m U) &= U \sum_{i=1}^n x_i^{m-1} a_i \cdot f(x_1) \cdots f(x_n) + f(x_1) \cdots f(x_n) U^2 = 0 \end{aligned}$$

and that all  $g_j(\beta), g_{m'-1}(\beta)$  and  $y_1 \cdots y_m U$  are antisymmetric in the  $x_i$ 's. □

Suppose now  $m = 2m'$  is even. Observe that the  $k$ -rational  $n$ -plane

$$X = \text{Span}\{(1, 0), \dots, (\beta^{n-m'-1}, 0), (g_0(\beta), 0), \dots, (g_{m'-2}(\beta), 0), (g_{m'-1}(\beta), y_1 \cdots y_m U)\}$$

is isotropic with respect to both quadratic forms. When  $m = 2$ , exclude  $(g_0(\beta), 0)$  and use  $(g_0(\beta), y_1 y_2 U)$  only. For later reference, we point out that the vector  $v = (\beta^{n-m'}, 0)$  lies in

$X_{Q_D}^\perp \setminus X$  with  $Q_D$ -norm 1. For each  $i = 1, \dots, m$ , the  $(n+1)$ -plane

$$Y_i = \text{Span}\{X, (h_i(\beta), 0)\}$$

is isotropic with respect to the quadratic form  $x_i Q_D - Q'_D$  corresponding to  $P_i$ . If  $Y_1$  lies in the ruling corresponding to  $\overline{P}_1$ , then  $\mathbb{P}X + (P_1) = -\mathbb{P}X_1$  where

$$\begin{aligned} X_1 = & \text{Span}\{(1, 0), \dots, (\beta^{n-m'-1}, 0), \\ & (g_0(\beta) - 2b_1 h_1(\beta), 0), \dots, (g_{m'-2}(\beta) - 2x_1^{m'-2} b_1 h_1(\beta), 0), \\ & (g_{m'-1}(\beta) - 2x_1^{m'-1} b_1 h_1(\beta), y_1 \cdots y_m U)\}, \end{aligned}$$

where  $b_i = a_i y_1 \cdots y_n / y_i$ .

If  $P_1$  is  $k$ -rational, then as in Example 2.40,  $(P_1) = (\overline{P}_1)$  in  $J(k)/2J(k)$ , so we don't need to worry about the case when  $Y_1$  lies in the ruling corresponding to  $P_1$ . If  $P_1$  is not  $k$ -rational, we proceed as in Example 2.43 and suppose  $P_2 = {}^\sigma P_1$  is one of its conjugate. To compute  $\mathbb{P}X + (P_1) + (P_2)$ , we need to find a  $n+1$  plane containing  $X$  in the ruling that doesn't contain  ${}^\sigma Y_1 = Y_2$ . The  $n+1$  plane

$$Y'_2 = \text{Span}\{X_1, (h_2(\beta), 0)\}$$

does the job as it intersects  $Y_2$  in codimension 1. From this we see  $\mathbb{P}X + (P_1) + (P_2) = \mathbb{P}X_2$  where

$$\begin{aligned} X_2 = & \text{Span}\{(1, 0), \dots, (\beta^{n-m'-1}, 0), (g_0(\beta) - 2b_1 h_1(\beta) - 2b_2 h_2(\beta), 0), \dots, \\ & (g_{m'-2}(\beta) - 2x_1^{m'-2} b_1 h_1(\beta) - 2x_2^{m'-2} b_2 h_2(\beta), 0), \\ & (g_{m'-1}(\beta) - 2x_1^{m'-1} b_1 h_1(\beta) - 2x_2^{m'-1} b_2 h_2(\beta), y_1 \cdots y_m U)\}, \end{aligned}$$

Let  $D_1 \in \text{Div}(C)(k)$  denotes the sum of the conjugates of  $(P_1)$ . If  $Y_1$  lies in the other ruling, then repeating the above procedure computes  $\mathbb{P}X + \overline{D}_1$  which differs from  $\mathbb{P}X + D_1$  by an element in

$2J(k)$  and thus is not of concern.

Repeating the above to exhaust  $D$ , one obtains, up to  $2J(k)$ ,

$$\begin{aligned}\mathbb{P}X + (P_1) + (P_2) + \cdots + (P_{2m'}) &= \mathbb{P}\text{Span}\{(1, 0), \dots, (\beta^{n-m'-1}, 0), (-g_0(\beta), 0), \dots, \\ &\quad (-g_{m'-2}(\beta), 0), (-g_{m'-1}(\beta), y_1 \cdots y_m U)\} \\ &= (\infty) - \mathbb{P}X.\end{aligned}$$

Rearranging gives the desired result.

Now for  $m = 2m' + 1$  odd, we take the  $k$ -rational  $n$ -plane

$$X = \text{Span}\{(1, 0), \dots, (\beta^{n-m'-2}, 0), (\beta^{n-m'-1}, 1), (g_0(\beta), 0), \dots, (g_{m'-2}(\beta), 0), (g_{m'-1}(\beta), 0)\}.$$

In this case, we can take  $v$  to be  $(g_{m'}(\beta), 0)$ . Likewise as above, we obtain

$$\begin{aligned}\mathbb{P}X + (P_1) + (P_2) + \cdots + (P_{2m'+1}) &= -\mathbb{P}\text{Span}\{(1, 0), \dots, (\beta^{n-m'-2}, 0), (\beta^{n-m'-1}, 1), \\ &\quad (-g_0(\beta), 0), \dots, (-g_{m'-2}(\beta), 0), (-g_{m'-1}(\beta), 0)\} \\ &= -\mathbb{P}X,\end{aligned}$$

as we claimed.

### 2.10.2 Case of a rational non-Weierstrass point

The computation in this case is the same as the above. We will just write down an  $X$  to keep the numerics straight.

Suppose  $[D] = (P_1) + \cdots + (P_m) - m_1(\infty) - (m - m_1)(\infty') \in J(k)$  with  $m$  minimal and  $P_i = (x_i, y_i)$ . The quadratic forms take the form,

$$\begin{aligned}Q_D(v) &= \text{Tr}((x_1 - \beta)(x_2 - \beta) \cdots (x_m - \beta)v^2 / f'(\beta)) \\ Q'_D(v) &= \text{Tr}((x_1 - \beta)(x_2 - \beta) \cdots (x_m - \beta)\beta v^2 / f'(\beta)).\end{aligned}$$

Define  $h_i(t), U, q_i, a_i, g_j(t)$  exactly as before.

- When  $m = 1$ , take

$$X = \text{Span}\{1, \beta, \dots, \beta^{n-1}\}.$$

- When  $m = 2$ , take

$$X = \text{Span}\{1, \beta, \dots, \beta^{n-2}, y_1 h_2(\beta) - y_2 h_1(\beta) + y_1 y_2 (x_1 - x_2) \beta^{n-1}\}.$$

- When  $m = 2m' + 1, m' \geq 1$ , take

$$X = \{1, \beta, \dots, \beta^{n-m'-1}, g_0(\beta), \dots, g_{m'-1}(\beta)\}.$$

- When  $m = 2m', m' \geq 2$ , take

$$X = \{1, \beta, \dots, \beta^{n-m'}, g_0(\beta), \dots, g_{m'-2}(\beta)\}.$$

### 3 Adelic approach to orbit counting

Recently Bhargava and Shankar proved in [5] that the average order of the 2-Selmer group of elliptic curves over  $\mathbb{Q}$  is 3 by counting certain orbits of binary quartic forms. In [2], Bhargava and Gross generalized the result to hyperelliptic curves of genus  $n$  over  $\mathbb{Q}$  with a marked rational Weierstrass point. They proved that the average order of the 2-Selmer group in this case is 3, independent of the genus. Once again the approach was by relating elements of the 2-Selmer group to the soluble orbits discussed in Chapter 2 followed by an analytic computation of the number of such orbits using the Bhargava-Shankar technique of geometry of numbers. In the case of elliptic curves, Poonen provided an adelic viewpoint to part of the orbit counting in [13].

The goal of this chapter is to complete this adelic analysis in a more abstract setting over an arbitrary number field. We will describe the setting via four sets of axioms. The goal at large is the computation of the average size of  $n$ -Selmer groups of certain families  $\mathcal{J}$  of abelian varieties, often arising as Jacobians of families of curves. Axioms I and II require the existence of a coregular representation of a semisimple reductive group with an identification of the stabilizers with the  $n$ -torsions of members of this family. Axiom IV requires the existence of a family of principal homogeneous spaces, one for each  $J \in \mathcal{J}$ . Axiom III is a condition on integral orbits so our adelic statements are not vacuous. This also corresponds to a “minimization” requirement needed in the sieves used in the Bhargava-Shankar technique of geometry of number. Thorne ([18]) found examples of families satisfying Axiom I and II.1 for the simple adjoint groups of type  $A, D, E$  and  $n = 2$ . Type  $A_{2g}$  corresponds to the family of hyperelliptic curves of genus  $g$  with a marked rational Weierstrass point, also known as “odd hyperelliptic curves”. Type  $A_{2g+1}$  corresponds to the family of hyperelliptic curves of genus  $g$  with a marked rational non-Weierstrass point, also known as “even hyperelliptic curves”. The cases  $n = 3, 4, 5$  for elliptic curves have been studied by Bhargava and his collaborators ([3],[4],[11]). We will show the above two families of hyperelliptic curves satisfy all four axioms using results from Chapter 2 extensively. More details on the application of this adelic analysis will follow after the statement of the main result Theorem 3.3 in Section 3.3 below.

### 3.1 Distinguished orbits

**Axiom I: (Coregularity)** Let  $G$  be a semisimple reductive group over  $k$  with a coregular linear representation  $V_0$  over  $k$  and geometric quotient  $S_0$ , such that

1. there exists a section  $\kappa : S_0 \rightarrow V_0$ , and
2. the map  $\delta : G \times S_0 \rightarrow V_0$  defined by  $\delta(g, f_0) = g \cdot \kappa(f_0)$  is étale.

Here **coregular** means the geometric quotient  $S_0$  is affine  $N$ -space for some  $N$ . For any field  $k'$  containing  $k$ , elements of  $V(k')$  lying in the image of  $\delta(G(k') \times S_0(k'))$  are said to be in the **distinguished orbits**. □

Let  $f$  denote the quotient map  $V_0 \rightarrow S_0$ . Viewing affine spaces as products of  $\mathbb{G}_a$ , one has left invariant top differential forms  $d\mu, d\nu, d\tau$  over  $k$  on  $S_0, V_0, G$ , unique up to  $k^\times$  scaling. Let  $d\tau \wedge d\mu$  denote the top form on  $G \times S_0$ .

**Lemma 3.1.**

$$\delta^* d\nu = c \cdot d\tau \wedge d\mu,$$

for some  $c \in k^\times$ .

**Proof:** (Jack Thorne) The measure  $d\nu$  on  $V_0$  is  $G$ -invariant because semisimple groups do not have non-trivial characters. Hence  $\delta^* d\nu / d\tau \wedge d\mu$  defines a regular function on  $S_0$ . Étale-ness implies that this function is nowhere vanishing, therefore must be constant since  $S_0 = \mathbb{A}^N$ . □

The baby example of a coregular representation is the adjoint representation of an adjoint simple group as a consequence of Chevalley's theorem. A more general source of example is Vinberg theory [19]. The section  $\kappa$  is the Kostant section and the étale condition is equivalent to

$$\dim G + \dim S_0 = \dim V_0. \tag{3.1}$$

We shall verify Axiom I for the two families of hyperelliptic curves we studied in Chapter 2, or rather the two representations we studied.

In the odd case, corresponding to hyperelliptic curves with a marked rational Weierstrass point, we had a  $2n + 1$  dimensional split quadratic space  $(U, <, >)$  of discriminant 1 over  $k$ , and the group  $G = \text{PO}_{2n+1}$  acting by conjugation on the space  $V_0$  of traceless self-adjoint operators  $T$  on  $U$ . The ring of polynomial invariants is the free polynomial ring generated by the coefficients of the characteristic polynomial. Therefore  $S_0 = \text{Spec}k[c_2, \dots, c_{2n+1}] = \mathbb{A}^{2n}$ . We shall view a  $k'$ -point of  $S_0$  as both the  $2n$ -tuple of coordinates and as the polynomial

$$f_0(x) = x^{2n+1} + c_2x^{2n-1} + \dots + c_{2n+1}.$$

This belongs to type  $A_{2n}$ -Vinberg satisfying (3.1). We will give a very explicit formula for the Kostant section in this case, mostly because we will be constructing similar (local) sections for the other orbits in the next section and it will help visualizing the easy case first.

Let  $e_0, \dots, e_{2n}$  be a basis for  $U$ , let  $R$  be any  $k$ -algebra, and let  $f_0 = (c_2, \dots, c_{2n+1}) \in S_0(R)$  be an  $R$ -point of  $S_0$ . Then  $\kappa(f_0)$  is the following operator  $T$  on  $U \otimes R$ :

$$\begin{aligned} T(e_i) &= e_{i+1}, \text{ for } i = 0, \dots, n-1, \\ T(e_n) &= e_{n+1} - \frac{1}{2}c_2e_{n-1}, \\ T(e_{n+i}) &= e_{n+i+1} - \frac{1}{2}c_{2i}e_{n-i+1} - c_{2i+1}e_{n-i} - \frac{1}{2}c_{2i+2}e_{n-i-1}, \text{ for } i = 1, \dots, n-1, \\ T(e_{2n}) &= -\frac{1}{2}c_{2n}e_1 - c_{2n+1}e_0. \end{aligned}$$

The above formula tells us if we were to do everything integrally, then  $\kappa$  is defined over  $\mathcal{O}_k[1/2]$ . This formula is obtained by working in the case  $R = k$ . Recall we had the  $2n + 1$  dimensional  $k$ -vector space

$$L = k[x]/(x^{2n+1} + c_2x^{2n-1} + \dots + c_{2n+1}) = k[\beta]$$

with a bilinear form  $<, >$  defined by

$$< \lambda, \mu > = \text{coefficient of } \beta^{2n} \text{ in } \lambda\mu.$$

The quadratic space  $(L, <, >)$  is split and we can construct a symplectic basis  $\{e_0, \dots, e_{2n}\}$ , in the sense  $\langle e_i, e_j \rangle = \delta_{i+j, 2n}$ , as follows:

$$\begin{aligned} e_i &= \beta^i, \text{ for } i = 0, \dots, n, \\ e_{n+1} &= \beta^{n+1} + \frac{1}{2}c_2\beta^{n-1}, \\ e_{n+i} &= \beta^{n+i} + c_2\beta^{n+i-2} + c_3\beta^{n+i-3} + \dots + c_{2i-1}\beta^{n-i+1} + \frac{1}{2}c_{2i}\beta^{n-i}, \text{ for } i = 2, \dots, n. \end{aligned}$$

Expressing the multiplication by  $\beta$  operator in this basis gives the above formula for  $T$ .

In the even case, for hyperelliptic curves with a marked rational non-Weierstrass point,  $(U, <, >)$  is now a  $2n + 2$  dimensional split quadratic space over  $k$  with the group  $G = \text{PSO}_{2n+2}$  acting by conjugation on the space  $V_0$  of traceless self-adjoint operators  $T$  on  $U$ . The geometric quotient is  $S_0 = \text{Spec} k[c_2, \dots, c_{2n+2}] = \mathbb{A}^{2n+1}$ . We shall view a  $k'$ -point of  $S_0$  as both the  $(2n+1)$ -tuple of coordinates and as the polynomial

$$f_0(x) = x^{2n+2} + c_2x^{2n} + \dots + c_{2n+2}.$$

This belongs to type  $A_{2n+1}$ -Vinberg satisfying (3.1). Let  $f_0 = (c_2, \dots, c_{2n+2}) \in S_0(k)$  be a  $k$ -point of  $S_0$ . Instead of writing down the formula for  $\kappa(f_0)$  as in the odd case, we will write down a symplectic basis  $\{e_0, \dots, e_{2n+1}\}$  for the quadratic space  $(L, <, >)$  where

$$L = k[x]/(x^{2n+1} + c_2x^{2n-1} + \dots + c_{2n+1}) = k[\beta]$$

and the bilinear form  $<, >$  is defined by

$$\langle \lambda, \mu \rangle = \text{coefficient of } \beta^{2n+1} \text{ in } \lambda\mu.$$



Recall  $\{e_0, \dots, e_{2n+1}\}$  is a symplectic basis if  $\langle e_i, e_j \rangle = \delta_{i+j, 2n+1}$ . We set,

$$\begin{aligned} e_i &= \beta^i, \text{ for } i = 0, \dots, n+1, \\ e_{n+i} &= \beta^{n+i} + c_2\beta^{n+i-2} + c_3\beta^{n+i-3} + \dots + c_{2i-2}\beta^{n-i+2} + \frac{1}{2}c_{2i-1}\beta^{n-i+1}, \text{ for } i = 2, \dots, n+1. \end{aligned}$$

Expressing the multiplication by  $\beta$  operator in this basis gives  $\kappa(f_0)$ . As we remarked in the odd case,  $\kappa$  can be defined over  $\mathcal{O}_k[1/2]$ .

### 3.2 Soluble orbits

**Axiom II.1: (Parametrization of the stabilizers)** There is a flat family of abelian varieties  $\mathcal{J}$  over an open subscheme  $S$  of  $S_0$  whose  $n$ -torsion<sup>2</sup> parametrizes the stabilizers for some  $n$ . More precisely, denote by  $V$  the open subscheme of  $V_0$  over  $S$ , then there is an injective morphism of  $V$ -schemes  $\mathcal{J}[n] \times_S V \rightarrow G \times V$  such that the image is precisely the stabilizer subscheme

$$\text{Stab}_k(G, V) = \{(g, T) | g.T = T\}.$$

Suppose further this morphism is  $G$ -equivariant where  $G$  acts on the left via  $V$  and on the right by  $g.(g_0, T) = (gg_0g^{-1}, g.T)$ .<sup>3</sup> □

For any  $f_0 \in S(k')$ , put  $T_0 = \kappa(f_0) \in V(k')$  and denote by  $J_{f_0}$  the fiber of  $\mathcal{J} \rightarrow S$  over  $f_0$ . Then there is an inclusion  $J_{f_0}[n] \hookrightarrow G$  identifying  $J_{f_0}[n]$  with  $\text{Stab}_G(T_0)$ . The collection of  $G(k')$ -orbits in  $G(k^s)T_0$  is in bijection with

$$\ker(H^1(k', J_{f_0}[n]) \rightarrow H^1(k', G)).$$

---

<sup>2</sup>This  $n$  is not to be confused with the  $n$  we used to denote the genus of the hyperelliptic curves. This  $n$  will be 2 in the hyperelliptic case.

<sup>3</sup>This last condition is not needed for Theorem 3.3, but will become convenient in Section 3.5.

**Axiom II.2: (Soluble orbits)** The following composite map is trivial

$$J_{f_0}(k')/nJ_{f_0}(k') \hookrightarrow H^1(k', J_{f_0}[n]) \rightarrow H^1(k', G).$$

The  $k'$ -orbits corresponding to classes coming from  $J_{f_0}(k')/nJ_{f_0}(k')$  are called the **soluble orbits**. Denote the subset of elements in  $V(k'), V_{f_0}(k')$  in the soluble orbits by  $V^s(k'), V_{f_0}^s(k')$ , respectively.  $\square$

The odd and even cases satisfy both of these two axioms. In both cases,  $S$  is the open subscheme consisting of  $f_0 \in S_0$  with non-zero discriminant, there is a family of hyperelliptic curves  $\mathcal{C} \rightarrow S$  where the fiber above  $f_0$  is the hyperelliptic curve defined by the affine equation  $y^2 = f_0(x)$ . Its relative  $\text{Pic}_{\mathcal{C}/S}^0$  is the abelian scheme  $\mathcal{J}$ . The identification of  $J_{f_0}[2]$  with the stabilizer subscheme has been done in Section 1.1 for the odd case and in Section 2.7 for the even case, with explicit formula for the map  $\mathcal{J}[2] \times_S V \rightarrow G$  given in Remark 1.6 and Remark 1.34. Axiom II.2 was verified in Theorem 2.5 and Theorem 2.20. This new definition of solubility coincides with the old definitions we saw in Chapter 2.

Suppose  $k'$  is a local field containing  $k$  of characteristic not dividing  $n$ . Fix any left-invariant Haar measure  $\mu$  on  $k'$ , for any  $c_0 \in k'$ , define  $|c_0|$  to be the positive real number such that  $\mu(c_0 E) = |c_0| \mu(E)$  for all measurable subset  $E \in k'$ . Since the quotient

$$\frac{|J_{f_0}(k')/nJ_{f_0}(k')|}{J_{f_0}[n](k')}$$

only depends on  $n, k'$  and the dimension of  $J_{f_0}$  hence independent of  $f_0 \in S(k')$ , and since  $\mathcal{J}[n]_{k'}$  is finite étale over  $S_{k'}$  from the assumption on the characteristic of  $k'$ , the number of soluble  $k'$ -orbits is locally constant over  $S(k')$ . The following axiom says that one can identify nearby soluble orbits via a local spreading.

**Axiom II.3: (Local spreading)** For any  $f_0 \in S(k'), [D] \in J_{f_0}(k')/nJ_{f_0}(k')$ , under the topology induced from  $|\cdot|$ , there exists a neighborhood  $U_0 \subset S(k')$  of  $f_0$  with a smooth map  $\epsilon_D : U_0 \rightarrow$

$G(k'^s)$ , as  $|\cdot|$ -adic manifolds, such that the rational orbit containing  $\epsilon_D(f_0)$  corresponds to the class  $[D]$  and the map  $\kappa_D : U_0 \rightarrow V(k'^s)$  defined by  $\kappa_D(f_1) = \epsilon_D(f_1)\kappa(f_1)$  factors through  $V(k')$ .  $\square$

To go from one  $G(k')$ -orbit to another  $G(k')$ -orbit, one needs to take an element  $g$  in  $G(k'^s)$ . The above axiom requires that one can select  $g$  continuously over  $U_0$ .

**Axiom II.4: (Local compatibility of measure)**<sup>4</sup> Combining  $\kappa_D$  with the group action gives a smooth map  $\delta_D : G(k') \times U_0 \rightarrow V(k')$ . Denote by  $\tau \times \mu$  the product measure on  $G(k') \times U_0$ , then

$$\delta_D^* \nu = |c| \tau \times \mu,$$

where the constant  $c$  comes from Axiom I.  $\square$

We shall verify these two axioms for the two cases we are mainly interested in. Consider the odd case first. Fix  $f_0 \in S(k')$  and fix any  $[D] \in J_{f_0}(k')/2J_{f_0}(k')$ , then  $[D]$  can be represented by a sum of points on the curve minus certain multiples of  $(\infty)$ . The coordinates of the points can be chosen to vary continuous in  $f_0 \in U_0$  by shrinking  $U_0$  if necessary. In fact, one can fix the  $x$ -coordinate and let the  $y$ -coordinate vary so the point lies on the new curve. Recall  $[D]$  gives rise to a class  $\alpha \in (L'^\times/L'^{\times 2})_{N=1}$  and a quadratic form  $\langle, \rangle_\alpha$  on  $L'$ . In Section 2.10, we constructed explicitly an isotropic  $n$ -dimensional  $k'$ -vector space  $X$  and a  $k'$ -rational vector  $v \in X^\perp \setminus X$  of norm 1 depending algebraically in the coordinates of the points representing  $[D]$ . In other words, the triple  $(L', X, v)$  varies continuously in the appropriate moduli space as  $f_0$  varies in  $U_0$ . Finally, the datum  $(L', X, v)$  determines algebraically an isometry  $L' \rightarrow U$ , and in (2.9) we saw how such an isometry determines a choice for  $g = \epsilon_D(f_1) \in G(k'^s)$ . Moreover, the image of the multiplication by  $\beta$  map gives  $\kappa_{[D]}(f_1)$ .

Note both  $\epsilon_D$  and  $\kappa_D$  are analytic and are defined by power series whose coefficients depend only on the coordinates of the initial collection of points. They are not defined by polynomial equations because we needed to take square roots. Let  $k'_1$  be a finite field extension of  $k'$  such

---

<sup>4</sup>Arul Shankar pointed out in a discussion that Axiom II.4 follows from Axiom II.3 and the Principle of permanence of identities.

that  $[D] \in 2J_{f_0}(k'_1)$ , let  $U_1$  denote the corresponding neighborhood of  $f_0$  in  $S(k'_1)$  in the same way  $U_0$  was defined in the above. By shrinking  $U_0$  and  $U_1$  if necessary, we see that the same power series define sections  $\kappa_D : U_0 \rightarrow V(k')$  and  $\kappa_D : U_1 \rightarrow V(k'_1)$ . Likewise  $\delta_D : G(k') \times U_0 \rightarrow V(k')$  and  $\delta_D : G(k'_1) \times U_1 \rightarrow V(k'_1)$  are defined by the same power series, hence they have the same Jacobian change of variable. The upshot is that in order to check Axiom II.4, it suffices to consider the case where  $\epsilon_D$  factors through  $G(k')$ . In this case,  $\delta_D$  factors as

$$\begin{aligned} G(k') \times U_0 &\rightarrow G(k') \times U_0 \xrightarrow{\delta} V(k') \\ (g, f_1) &\mapsto (g \cdot \epsilon_D(f_1), f_1) \end{aligned}$$

The first map has unit Jacobian as the left Haar measure on  $G$  is also right invariant, the second map has Jacobian  $c$  by Axiom I. Taking  $|\cdot|$  of the Jacobian gives the constant  $|c|$  as required by Axiom II.4.

The even case is almost exactly the same except we should mention a bit of extra caution in defining  $\epsilon_D$  and the local section  $\kappa_D$  associated to some  $[D] \in J_{f_0}(k')/2J_{f_0}(k')$ . Let  $g_{Y_0}$  denote an element of  $\text{PO}_{2n+2}(k)$  not in  $\text{PSO}_{2n+2}(k)$ , for example the reflection about any rational hyperplane. When  $(\infty) - (\infty')$  is not divisible by 2 in  $J_{f_0}(k')$ , we choose a set of representatives  $[D] \in J_{f_0}(k')$  for  $J_{f_0}(k')/\langle 2J_{f_0}(k'), (\infty) - (\infty') \rangle$  and define  $\epsilon_D$  and  $\kappa_D$  as usual. We define  $\epsilon_{[D]+(\infty)-(\infty')}$  by post-composing  $\epsilon_D$  with left multiplication by  $g_{Y_0}$  and define  $\kappa_{[D]+(\infty)-(\infty')}$  by post-composing  $\kappa_D$  with conjugation by  $g_{Y_0}$ .

Before moving on to state the main theorem, we point out that Axiom II.3 and II.4 allows us to compute measures of subsets in  $V^s(k')$  fiberwise. More precisely,

**Proposition 3.2.** Assuming Axiom II.3. There exist a measure  $\tau_{f_0}$  on  $V_{f_0}^s(k')$  for every  $f_0 \in S(k')$  such that for any measurable subset  $E \subset V^s(k')$ ,

$$\nu(E) = \int_{f(E)} \tau_{f_0}(E_{f_0}) df_0, \tag{3.2}$$

where  $E_{f_0}$  denotes the fiber of  $E$  over  $f_0$ .

**Proof:** Fix  $f_0 \in S(k')$ . The images of  $\delta_D$  as  $[D]$  varies in  $J_{f_0}(k')/2J_{f_0}(k')$  are disjoint and sweep out the entire  $V^s(k') \cap f^{-1}(U_0)$ . Let  $\delta_{f_0}$  denote the map  $G(k') \rightarrow V(k')$  sending  $g$  to  $\delta_D(g, f_0)$ . Denote its image by  $V_{f_0,D}$ , then

$$V_{f_0}^s(k') = \coprod_{D \in J_{f_0}(k')/2J_{f_0}(k')} V_{f_0,D}.$$

We define  $\tau_{f_0}$  on  $V_{f_0}$  as a sum of measures  $\tau_{f_0,D}$  on  $V_{f_0,D}$ . For any  $E \subset V_{f_0,D}$  and any open ball  $U_\epsilon$  around  $f_0$  of radius  $\epsilon$  inside  $U_0$ , we spread  $E$  out by taking

$$E_\epsilon = \delta_D(\delta_{f_0}^{-1}(E) \times U_\epsilon) \subset V(k').$$

We say  $E$  is  $\tau_{f_0,D}$ -measurable if  $E_\epsilon$  is  $\nu$ -measurable for small enough  $\epsilon$  and define

$$\tau_{f_0,D}(E) = \lim_{\epsilon \rightarrow 0+} \frac{\nu(E_\epsilon)}{\mu(U_\epsilon)}.$$

From the way it is defined, it is clear that (3.2) is satisfied. Note we didn't need Axiom II.4 to know the limit exists. A priori, there is a continuous non-negative real-valued function  $c_D$  on  $U_0$  such that

$$\delta_D^* \nu = c_D \tau \times \mu.$$

Then

$$\begin{aligned} \nu(E_\epsilon) &= \frac{\tau(\delta_{f_0}^{-1}(E))}{|\text{Stab}_G(\kappa_D(f_0))(k')|} \cdot \int_{U_\epsilon} c_D(s) ds \\ \tau_{f_0,D}(E) &= \frac{\tau(\delta_{f_0}^{-1}(E))}{|\text{Stab}_G(\kappa_D(f_0))(k')|} \cdot c_D(f_0). \end{aligned}$$

Axiom II.4 tells us that  $c_D$  is the constant  $|c|$ , independent of  $[D]$ . □

### 3.3 Statement of the Main Theorem and integral orbits

We are now set for stating the main result of our Main Theorem, though not the hypotheses.

**Theorem 3.3.** Suppose  $k$  is a number field. For each finite place  $\nu$ , let  $\mathcal{O}_\nu$  denote the local ring of integers. Let  $K$  be a measurable subset of  $S(\prod_{\nu \neq \infty} \mathcal{O}_\nu \times \prod_{\nu | \infty} k_\nu)$  of finite measure. Let  $V_K \subset V(\mathbb{A}_k)$  be its soluble preimage. That is  $V_K$  is the intersection in  $V(\prod k_\nu)$  of  $f^{-1}(K)$ ,  $V(\mathbb{A}_k)$  and

$$V^{ls} = \{(T_\nu)_\nu | T_\nu \text{ is in a soluble } k_\nu \text{ orbit, } \forall \nu\}.$$

Suppose Axioms I, II, III, IV are satisfied, then

$$\nu(G(k) \backslash V_K) = \tau(G(k) \backslash G(\mathbb{A}_k)) \cdot \mu(K), \quad (3.3)$$

where the left hand side is computed by taking the measure of a measurable fundamental set.

In practice, how will one apply this Theorem? The main question we are trying to answer is the average order of the  $n$ -Selmer group of a certain family of abelian varieties  $\mathcal{J}$ . Over  $k_\nu$ , for a fixed  $f_\nu \in S(k_\nu)$ , there is a bijection between soluble orbits over  $f_\nu$  and  $J_{f_\nu}(k_\nu)/nJ_{f_\nu}(k_\nu)$  by definition. For any  $f_0 \in S(k)$ , if  $G$  satisfies the Hasse principle, then there is a bijection between classes in  $\text{Sel}_n(k, J_{f_0})$  and  $G(k)$ -orbits over  $f_0$  that are everywhere locally soluble.

$$\begin{array}{ccccc} \text{Sel}_n(k, J_{f_0}) & \hookrightarrow & H^1(k, J_{f_0}[n]) & \longrightarrow & H^1(k, G) \\ & & \downarrow & & \downarrow \text{Hasse Principle} \\ \prod_\nu J_{f_0}(k_\nu)/nJ_{f_0}(k_\nu) & \longrightarrow & \prod_\nu H^1(k_\nu, J_{f_0}[n]) & \longrightarrow & \prod_\nu H^1(k_\nu, G) \end{array}$$

That is, there is a bijection

$$\text{Sel}_n(k, J_{f_0}) \longleftrightarrow G(k) \backslash V_{f_0}^s(k).$$

Suppose one has a notion of “height” on the family  $\mathcal{J}$ , denoted by  $H(J)$ , or  $H(C)$  if  $\mathcal{J}$  is the picard scheme of a family of curves. For positive real number  $X$ , one uses the theory of adelic geometry of numbers to choose a measurable subset  $S(\mathbb{A}_k)_{<X} = K_X$  of  $S(\prod_{\nu \neq \infty} \mathcal{O}_\nu \times \prod_{\nu | \infty} k_\nu)$

such that the following two comparisons hold.

$$\mu(S(\mathbb{A}_k)_{<X}) \sim \sum_{H(J)<X} 1. \quad (3.4)$$

$$\nu(G(k) \backslash V_{K_X}) \sim \sum_{H(J)<X} (\#\text{Sel}_n(k, J) - \gamma), \quad (3.5)$$

for some integer  $\gamma$  obtained using Bhargava-Shankar's technique of point counting in truncated fundamental domains.

Then applying the above comparison Theorem tells us the average order of the  $n$ -Selmer group of the family  $\mathcal{J}$  is  $\tau_G + \gamma$ , where  $\tau_G$  is the Tamagawa number of  $G$ .

For the family of hyperelliptic curves with a marked rational Weierstrass point,  $\tau_{PO} = 2$  and we expect that  $\gamma$  is 1 corresponding to the trivial class. Therefore the average order of the 2-Selmer group is expected to be 3 over an arbitrary number field, generalizing the work of Bhargava and Gross [2]. For the family of hyperelliptic curves with a marked rational non-Weierstrass point,  $\tau_{PSO} = 4$  and we expect that  $\gamma$  is 2 corresponding to the trivial class and the class  $(\infty) - (\infty')$ . Therefore the average order of the 2-Selmer group is expected to be 6 over arbitrary number field in this case.

The heuristic for Theorem 3.3 is that if  $G$  acts simply-transitively on  $V$ , then just the level of comparison of measure in Lemma 3.1 is enough. In the general case, the size of each stabilizer is the same as the number of soluble orbits away from a finite number of places. Over the bad places, the total number of them also match up due to the following product formula of Tate for abelian varieties

$$\prod_{\nu} \frac{|J(k_{\nu})/nJ(k_{\nu})|}{|J[n](k_{\nu})|} = 1. \quad (3.6)$$

Proposition 3.2 says one can compute measures in the soluble part fiberwise over a field. However, the naive approach of extending Proposition 3.2 to adèles fails because there are infinitely many adelic orbits with infinite adelic stabilizers. The actual approach we take involves “straightening” out  $V$  using torsors of  $\mathcal{J}$  and defining two adelic measures on this bigger space one of which

computes the left hand side of (3.12) by definition, while the other one computes the right hand side of (3.12) very easily. We will show that these two measures are equal, and not surprisingly, (3.6) is needed.

Before the straightening process, we need to discuss the integral orbits of the action of  $G$  on  $V$ . A priori it is not clear that  $V_K$  maps surjectively to  $K$ . Suppose  $k$  is a number field.

**Axiom III.1: (Integral  $V$ )** For almost all finite places  $\nu$ , every rational soluble orbit contains an integral orbit, that is, if  $T \in V^s(k_\nu)$  with  $f(T) \in S(\mathcal{O}_\nu)$ , then there exists  $g \in G(k_\nu)$  such that  $g.T \in V(\mathcal{O}_\nu)$ .  $\square$

**Axiom III.2: (Integral  $G$ )** For almost all finite places  $\nu$ , let  $S'_\nu \subset S(\mathcal{O}_\nu)$  be the collection of  $f_\nu$  such that if  $g \in G(k_\nu)$ ,  $T_1, T_2 \in V_{f_\nu}^s(\mathcal{O}_\nu)$ ,  $g.T_1 = T_2$ , then  $g \in G(\mathcal{O}_\nu)$ . Define

$$S' = \{(f_\nu)_\nu \mid f_\nu \in S'_\nu \text{ for almost all finite } \nu\} \subset S(\prod_{\nu \neq \infty} \mathcal{O}_\nu). \quad (3.7)$$

Then  $\mu(S') = \mu(S(\prod_{\nu \neq \infty} \mathcal{O}_\nu))$ .  $\square$

Notice Axiom III.2 is equivalent to the following axiom.

**Axiom III.2':** For almost all finite places  $\nu$ , there exists a measurable subset  $S'_\nu \subset S(\mathcal{O}_\nu)$  such that

**(Uniqueness)** If  $f_\nu \in S'_\nu$ , then every rational soluble orbit over  $f_\nu$  contains a unique integral orbit.

**(Integral stabilizer)** If  $f_\nu \in S'_\nu$  and  $T \in V_{f_\nu}^s(\mathcal{O}_\nu)$ , then  $\text{Stab}_G(T)(k_\nu) \subset G(\mathcal{O}_\nu)$ .

**(Full measure)** Define  $S'$  as in (3.7), then  $\mu(S') = \mu(S(\prod_{\nu \neq \infty} \mathcal{O}_\nu))$ .  $\square$

To check these for the representations of PO and PSO, we give some equivalent criterions for integrality. Recall the set up of  $V$  being the collection of trace-less self-adjoint operators on a split quadratic space  $(U, <, >)$  of discriminant 1. The dimension of  $U$  is either  $2n + 1$  or



$2n + 2$  depending on which case we are in. A **lattice** in  $U$  is a free  $\mathcal{O}_\nu$ -submodule  $M$  of full rank, namely such that  $U = M \otimes_{\mathcal{O}_\nu} k_\nu$ . A lattice  $M$  is **self-dual** if

$$M = M^\wedge = \{m' \in U \mid \langle m, m' \rangle \in \mathcal{O}_\nu, \forall m \in M\}.$$

An operator  $T \in V(k_\nu)$  is **integral** if there is a self-dual lattice  $M$  in  $U$  invariant under  $T$ .

When  $\nu \nmid 2$ , there is an alternative definition described in [2] Section 8. View  $f_0 \in S(\mathcal{O}_\nu)$  as the polynomial it corresponds to, define  $L = k_\nu[x]/f_0$  and  $R = \mathcal{O}_\nu[x]/f_0$ , and let  $\beta$  denote the image of  $x$ . For any  $T \in V_{f_0}(k_\nu)$ , up to conjugation by  $g_{Y_0}$  in the even case, there exists  $\alpha \in L^\times$  with square norm to  $k$  such that  $T$  is the image of the multiplication by  $\beta$  map under a  $k$ -isometry from  $(L, \langle, \rangle_\alpha)$  to  $(U, \langle, \rangle)$ . Recall  $\langle, \rangle_\alpha$  is defined by

$$\langle \lambda, \mu \rangle_\alpha = \text{coefficient of } \beta^{2n} \text{ or } \beta^{2n+1} \text{ in } \alpha \lambda \mu.$$

The existence of a self-dual lattice  $M$  translates into the existence of a fractional ideal  $I$  of  $R$  such that  $\alpha I^2 = R$ . Then Axiom III.1 follows from the following Proposition of [2].

**Proposition 3.4.** ([2] Proposition 16) If the class of  $\alpha$  in  $(L^\times/L^{\times 2})_{N=1}$  (odd case) or  $(L^\times/L^{\times 2}k^\times)_{N=1}$  (even case) lies in the image of  $J_{f_0}(k_\nu)/2J_{f_0}(k_\nu)$ , then  $I$  exists.

**Proof:** The proof in [2] focuses on  $k = \mathbb{Q}$  and deals with the odd case. It works verbatim in our more general case, but we will include some of the key points here. Suppose  $\alpha$  is given by the rational divisor

$$[D] = (P_1) + \cdots + (P_m) - m(\infty),$$

where  $P_i = (a_i, b_i)$  is integral in some finite field extension of  $k_\nu$  and  $m \leq n$ . Since we only care about the image of  $[D]$  under the Kummer map, we might as well forget the other point at infinity in the even case. Also, since the curve has a rational point, it is only a priori clear that the above expression for  $[D]$  is possible without the bound on  $m$ . Let  $R(x) \in k_\nu[x]$  be the monic

polynomial of degree  $m - 1$  such that for all  $i$ ,  $R(a_i) = b_i$  and let

$$P(x) = (x - a_1) \cdots (x - a_m) \in \mathcal{O}_\nu[x].$$

Now  $P(x)$  divides  $R(x)^2 - f(x)$  in  $k_\nu[x]$ . If  $m > n$ , then the quotient  $(R(x)^2 - f(x))/P(x) = Q(x)$  is a polynomial of degree  $m - 2$  unless  $m = n + 1$  and we are in the even case in which case it has degree  $m - 1$ . Therefore replacing  $[D]$  by  $\text{div}(y - R(x)) - [D]$  always cuts down  $m$ .

As we will show in Lemma 3.5 below, we can further assume that all the  $b_i$  are nonzero. Then  $\alpha = (-1)^m P(\beta)$ . If the polynomial  $R(x) \in \mathcal{O}_\nu[x]$ , then the ideal  $I = (1, R(\beta)/\alpha)$  does the job. Note  $\alpha I^2 = (\alpha, R(\beta), Q(\beta))$ . The integrality assumption of  $R(x)$  is used to show that  $R(\beta), Q(\beta) \in R$ . A computation of ideal norms shows that  $\alpha I^2 = R$ .

When  $R(x)$  is not integral, a Newton polygon analysis on  $f(x) - R(x)^2$  shows that there is a divisor class  $[D'] \in J_{f_0}(k_\nu)$  of the form  $(P'_1) + \cdots + (P'_{m-2}) - (m - 2)(\infty)$  differing from  $[D]$  by an element in  $2J_{f_0}(k_\nu)$ . One may apply induction on  $m$  to finish the argument.  $\square$

**Lemma 3.5. (Horizontal Moving Lemma)**<sup>5</sup> Let  $C$  be a hyperelliptic curve over  $k_\nu$  of genus  $g$  defined by the affine equation  $y^2 = f_0(x)$  where  $f_0 \in \mathcal{O}_\nu[x]$  is a monic polynomial of degree  $N$ . Let  $\alpha_1, \dots, \alpha_N$  denote the roots of  $f_0$  and let  $(P_1) = (\alpha_1, 0), \dots, (P_N) = (\alpha_N, 0)$  denote the corresponding Weierstrass points. Suppose  $[D] = (P_1) + \dots + (P_r) - r(\infty) \in J(k_\nu)$  for some  $r \leq N$ , then there exists another divisor class  $[D']$  with at most  $r$  points in its support away from  $\infty$ , none of which equals to  $P_i$  for some  $i$ , such that the images of  $[D]$  and  $[D']$  in  $L^\times/L^{\times 2}$  or  $L^\times/L^{\times 2}k^\times$  coincide.

**Proof:** By replacing  $[D]$  with  $(P_{r+1}) + \cdots + (P_N) - (N - r)(\infty)$  if necessary, we assume  $r \leq N/2$ . We also assume that  $\alpha_1, \dots, \alpha_r$  are all the conjugates of  $\alpha_1$  over  $k_\nu$ . Let  $g_0(x)$  be the minimal polynomial of  $\alpha_1$ . Then  $f_0(x)$  factors as  $f_0(x) = g_0(x)g(x)$  with  $g(x)$  monic of degree

---

<sup>5</sup>In some sense the Newton polygon argument can be viewed as the Vertical Moving Lemma.

$d = N - r \geq r$ . Let  $\pi$  denote the uniformizer in  $k_\nu$ . Consider the divisor

$$\operatorname{div}(y - \pi \prod_{i=1}^r (x - \alpha_i)) = (P_1) + \cdots + (P_r) + (Q_1) + \cdots + (Q_d) - N(\infty),$$

where  $Q_i \in C(k_\nu^s)$  and their  $x$ -coordinates are the roots of the polynomial

$$h(x) := g(x) - \pi^2 \prod_{i=1}^r (x - \alpha_i) = u \prod_{i=1}^d (x - b_i),$$

for some unit  $u$  in the case  $N = 2n + 2 = 2r = 2d$ . Write  $L_0 = k_\nu[x]/(g_0(x))$ ,  $L_1 = k_\nu[x]/(g(x))$  with generators  $\beta_0, \beta_1$ . Then as an element of  $(L_0^\times/L_0^{\times 2}) \times (L_1^\times/L_1^{\times 2})$ , or further modding out by the diagonal  $k_\nu^\times$  in the even case,

$$\begin{aligned} \operatorname{image}([D]) &= \operatorname{image}((Q_1) + \cdots + (Q_d) - d(\infty)) \\ &= \left( \prod_{i=1}^d (b_i - \beta_0), \prod_{i=1}^d (b_i - \beta_1) \right) \\ &= ((-1)^d h(\beta_0), (-1)^d h(\beta_1)) \\ &= ((-1)^d g(\beta_0), (-1)^{d+1} \pi^2 \prod_{i=1}^r (\beta_1 - \alpha_i)) \\ &= ((-1)^{r+1} g(\beta_0), \prod_{i=1}^r (\alpha_i - \beta_1)). \end{aligned}$$

We seek an  $r$ -tuple  $(x_1, \dots, x_r)$  satisfying the following conditions

1.  $x_1, \dots, x_r$  are conjugates of each other.
2.  $(-1)^{r+1} (\prod_{i=1}^r (x_i - \beta_0)) / g(\beta_0)$  is a square in  $L_0^\times$ .
3.  $\prod_{i=1}^r ((x_i - \beta_1) / (\alpha_i - \beta_1))$  is a square in  $L_1^\times$ .

It turns out from the construction below that  $f(x_i) = g_0(x_i)g(x_i)$  is a square in  $k_\nu(\alpha_1, \dots, \alpha_r)^\times$  for all  $i$ .

Define for each  $i = 1, \dots, r$

$$q_i = \prod_{1 \leq j \leq r, j \neq i} (\alpha_j - \alpha_i) \quad (3.8)$$

$$x_i = \alpha_i + (-1)^{r+1} q_i g(\alpha_i) \pi^M \quad (3.9)$$

where  $M$  is a sufficiently large even integer. Condition 1 is clearly satisfied and 3 is also if  $q_i g(\alpha_i) \pi^M / (\alpha_i - \beta_1)$  has positive valuation. To check condition 2, we make many uses of the identity  $\prod_{i=1}^r (\alpha_i - \beta_0) = 0$ . Indeed, we have

$$\begin{aligned} (-1)^{r+1} \prod_{i=1}^r (x_i - \beta_0) &= (-1)^{r+1} \prod_{i=1}^r (a_i - \beta_0 + \pi^M (-1)^{r+1} q_i g(a_i)) \\ &= \pi^M \sum_{i=1}^r \left( q_i g(a_i) \prod_{j \neq i} (a_j - \beta_0) \right) + \text{higher valuation terms,} \end{aligned}$$

Focusing on the important piece, we have

$$\begin{aligned} \sum_{i=1}^r \left( q_i g(\alpha_i) \prod_{j \neq i} (\alpha_j - \beta_0) \right) &= \sum_{i=1}^r \left( (g(\beta_0) + (\alpha_i - \beta_0) \cdot (\text{stuff})) \prod_{j \neq i} ((\alpha_j - \alpha_i)(\alpha_j - \beta_0)) \right) \\ &= g(\beta_0) \sum_{i=1}^r \prod_{j \neq i} ((\alpha_j - \beta_0 + \beta_0 - \alpha_i)(\alpha_j - \beta_0)) \\ &= g(\beta_0) \sum_{i=1}^r \prod_{j \neq i} (\alpha_j - \beta_0)^2 \\ &= g(\beta_0) \left( \sum_{i=1}^r \prod_{j \neq i} (\alpha_j - \beta_0) \right)^2, \end{aligned}$$

which after dividing by  $g(\beta_0)$  becomes a square in  $L_0^\times$ , confirming condition 2. Once again the smoothness of  $C$  ensured that  $x_i \neq \alpha_i$ , and by enlarging  $M$  if necessary,  $x_i \neq \alpha_j$  for any  $j$ . The proof of the Moving Lemma is now complete, and moreover, one can compute, modulo squares

in  $k(\alpha_1, \dots, \alpha_r)^\times$ ,

$$\begin{aligned}
f(x_i) &= \left( \prod_{j=1}^r (x_i - \alpha_j) \right) g(x_i) \\
&= \left( (-1)^{r+1} q_i g(\alpha_i) \pi^M \prod_{j \neq i} (\alpha_i - \alpha_j + \pi^M(\text{stuff})) \right) (g(\alpha_i) + \pi^M(\text{stuff})) \\
&= (-1)^{r+1} q_i g(\alpha_i)^2 \pi^M (-1)^{r-1} \prod_{j \neq i} (\alpha_j - \alpha_i) \\
&= q_i^2 g(\alpha_i)^2 \pi^M \\
&\in k(\alpha_1, \dots, \alpha_r)^{\times 2}. \quad \square
\end{aligned}$$

To check Axiom III.2', we define for each  $\nu \nmid 2$ ,

$$S'_\nu = \{f_\nu \in S(\mathcal{O}_\nu) \mid \text{val}_\nu(\text{disc}(f_\nu)) \leq 1\}.$$

If  $f_\nu \in S'_\nu$ , then  $R = \mathcal{O}_\nu[x]/f_\nu$  is the maximal order, and uniqueness of integral orbits inside one rational orbit follows from [2] Corollary 14.

Suppose now  $T \in V^s(\mathcal{O}_\nu)$  over  $f_\nu \in S'_\nu$ , and suppose  $g \in \text{Stab}_G(T)(k_\nu)$ . Let  $\alpha_1, \dots, \alpha_{2n+1}$  or  $\alpha_{2n+2}$  denote the roots of  $f_\nu$ . Recall the discriminant of  $f_\nu$  is defined by

$$\text{disc}(f_\nu) = \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

The explicit description of  $\text{Stab}_G(T)$  in Remark 1.6 and Remark 1.34 tells us  $g$  is of the form

$$1 - 2 \sum_{i \in I} \frac{h_i(T)}{h_i(\alpha_i)},$$

for some subset  $I \subset \{1, \dots, 2n+2\}$  and where  $h_i(x) =: f(x)/(x - \alpha_i)$ . Observe that  $\text{lcm}_{i \in I} h_i(\alpha_i) \in \mathcal{O}_\nu$  and its square divides the discriminant. Therefore it must be a unit in  $\mathcal{O}_\nu$  and  $g \in G(\mathcal{O}_\nu)$ .

Finally, for each finite  $\nu$ , let  $\mu_\nu$  denote the local measure on  $S(k_\nu)$ . Then for almost all  $\nu$ ,

Weil's formula says

$$\mu_\nu(S'_\nu) = \mu_\nu(S(\mathcal{O}_\nu))(1 - (N\nu)^{-2} + o((N\nu)^{-3})). \quad (3.10)$$

For any finite subset  $I$  of the places of  $k$  that contains all the infinite places, places where (3.10) does not hold, define

$$S'_I = \prod_{\nu \in I} S(\mathcal{O}_\nu) \times \prod_{\nu \notin I} S'_\nu.$$

Then each  $S'_I$  is measurable and  $S' = \cup_I S'_I$  is also measurable. Moreover,

$$\mu(S') \geq \mu(S'_I) = \mu(S(\prod_{\nu \notin I} \mathcal{O}_\nu)) \prod_{\nu \notin I} (1 - (N\nu)^{-2} + o((N\nu)^{-3})).$$

The product converges to 1 as  $I$  increases. Hence,  $\mu(S') = \mu(S(\prod_{\nu \notin \infty} \mathcal{O}_\nu))$ .

Therefore, the two cases we are primarily interested in satisfy Axiom III. So far, all three axioms are centered around the representation theoretic aspect. The last set of axioms focuses on torsors of the abelian scheme  $\mathcal{J}$ .

### 3.4 Straightening

**Axiom IV: (Torsor of  $\mathcal{J}$ )** Let  $W \xrightarrow{\pi} V$  be a torsor for  $\mathcal{J} \times_S V$  as a  $V$ -scheme, such that

1.  $G$  acts on  $W$  equivariantly with respect to  $\pi$ ,
2. there is a section  $\kappa_W : S \rightarrow W$  extending the section  $\kappa$ , that is  $f \circ \kappa_W = \kappa$ ,
3. the actions of  $G \times V$  and  $\mathcal{J} \times_S V$  on  $W$  commute and coincide on the common  $\mathcal{J}[n] \times_S V$ , that is the following two diagrams commute,

$$\begin{array}{ccc} G \times \mathcal{J} \times_S W & \xrightarrow{\quad} & G \times W \\ \downarrow & & \downarrow \\ \mathcal{J} \times_S G \times W & \longrightarrow & \mathcal{J} \times_S W \longrightarrow W \end{array} \quad \begin{array}{ccc} \mathcal{J}[n] \times_S V \times_V W & \longrightarrow & G \times V \times_V W \\ \downarrow & & \downarrow \\ \mathcal{J} \times_S W & \longrightarrow & W \end{array}$$

4. for any field  $k'$  containing  $k$ ,  $\pi(W(k')) = V^s(k')$ .

□

When  $k$  is a number field and  $\nu$  is a finite place, we define  $W(\mathcal{O}_\nu)$  as  $\pi^{-1}(V(\mathcal{O}_\nu))$ .

We first verify this axiom in our hyperelliptic cases since this axiom might seem fairly artificial at the moment.

For the odd case,  $W$  is a closed subscheme of  $V \times \mathbb{G}r(n, U \oplus k)$ . For any  $k$ -algebra  $R$ ,  $W_0(R)$  is the collection of pairs  $(T, X)$  with  $T \in V_0(R)$ , and  $X$  a free sub- $R$ -module of rank  $n$  in  $(U \otimes R) \oplus R$  such that for any  $x, x' \in X$ ,  $Q_0(x, x') = 0 = Q_T(x, x')$ , where  $Q_0$  and  $Q_T$  are two quadratic forms on  $(U \otimes R) \oplus R$  defined as follows over  $k$ ,

$$\begin{aligned} Q_0(u, w) &= \langle u, u \rangle \\ Q_T(u, w) &= \langle u, Tu \rangle + w^2, \end{aligned}$$

for  $u \in U, w \in k$ . As we have seen in Section 2.4, the fibers of  $W \rightarrow V$  form torsors of the corresponding Jacobians. One has the following action of  $\mathcal{J}$  on  $W$ ,

$$\begin{aligned} (\mathcal{J} \times_S V) \times_V W &= \mathcal{J} \times_S W \rightarrow W \\ ([D], T, X) &\mapsto (T, X + [D]), \end{aligned}$$

where one can view the above  $+$  as either the action of  $J$  on the fiber, or as the addition in the disconnected group discussed in Chapter 1. Since  $[D]$  is 2-torsion,  $X + [D] = X - [D]$  and the latter definition will be used in the general case.

The section  $\kappa_W$  is constructed by taking  $\kappa$  for the first coordinate, and by taking the image of  $\text{Span}\{e_0, \dots, e_{n-1}\}$  for the second coordinate where  $\{e_0, \dots, e_{2n}\}$  is the symplectic basis obtained in Section 3.1. The group  $G = \text{PO}_{2n+1}$  acts on  $U \oplus k$  via the normal action on  $U$  and via the identity on  $k$ . Therefore it acts on  $W$  via  $g.(T, X) = (gTg^{-1}, gX)$ . It follows directly from the definition of the action of the Jacobian that the actions of  $G$  and  $\mathcal{J}$  commute. To show they agree on the common  $\mathcal{J}[2] \times_S V$ , we look at the fiber  $F_T$  of  $W \rightarrow V$  above some  $T \in V$ . Let  $J$  denote the corresponding Jacobian. For  $[D] \in J$ , denote by  $\alpha([D]) : F_T \rightarrow F_T$  its action on the fiber. For  $[E] \in J[2]$ , denote by  $\beta([E]) : F_T \rightarrow F_T$  the action coming from  $G$ . We already

know from Proposition 2.7 that  $\alpha([E]), \beta([E])$  coincide on a nonempty subscheme of  $F_T$ , namely  $F_T[2]_\infty$ . Transitivity of the action of  $J$  on  $F_T$  and the commutativity of the first diagram allow us to propagate this equality to all of  $F_T$ . Finally Axiom IV.4 was the content of Theorem 2.5.

For the even case,  $U$  has dimension  $2n+2$ ,  $W$  is a closed subscheme of  $V \times \mathbb{G}r(n, U)$ . For any  $k$ -algebra  $R$ ,  $W_0(R)$  is the collection of pairs  $(T, X)$  with  $T \in V_0(R)$ , and  $X$  a free sub- $R$ -module of rank  $n$  in  $U \otimes R$  such that for any  $x, x' \in X$ ,  $Q_0(x, x') = 0 = Q_T(x, x')$ , where  $Q_0$  and  $Q_T$  are two quadratic forms on  $U \otimes R$  defined as follows over  $k$ ,

$$\begin{aligned} Q_0(u) &= \langle u, u \rangle \\ Q_T(u) &= \langle u, Tu \rangle. \end{aligned}$$

Axiom IV follows from the parallel discussion in the second half of Chapter 2.

We now work towards the proof of Theorem 3.3. Assume all four sets of axioms are satisfied.

Commutativity of the actions of  $G$  and  $\mathcal{J}$  gives an action of  $G \times \mathcal{J}$  on  $W$  over  $S$ . Observe that one can embed  $\mathcal{J}[n] \times_S W$  diagonally in  $G \times \mathcal{J} \times_S W$ . From the identification of  $\mathcal{J}[n] \times_S V$  as the stabilizer subscheme of the action of  $G$  on  $V$  in Axiom II.1, and the fact that  $W$  is a  $\mathcal{J}$ -torsor over  $V$ , one can identify  $\mathcal{J}[n] \times_S W$  with  $\text{Stab}_S(G \times \mathcal{J}, W)$  via the above embedding.

Using the section  $\kappa$ , we get a morphism

$$\iota : \mathcal{J}[n] \xrightarrow{\kappa} \mathcal{J}[n] \times_S V \rightarrow G \times V \rightarrow G.$$

It allows us to embed  $\mathcal{J}[n]$  diagonally as a finite subgroup scheme of  $G \times \mathcal{J}$ . The above identification allows us to define the following map,

$$\gamma : \frac{G \times \mathcal{J}}{\mathcal{J}[n]} \xrightarrow{\text{id} \times \kappa_W} \frac{G \times \mathcal{J}}{\mathcal{J}[n]} \times_S \kappa_W(S) \rightarrow W. \quad (3.11)$$

More concretely, let  $k'$  be a field over  $k$  and for any  $f_0 \in S(k')$ , let  $W_{f_0}, J_{f_0}$  denote the fibers of  $W \rightarrow S, \mathcal{J} \rightarrow S$  over  $f_0$ . View  $J_{f_0}[n]$  as a subgroup of  $G$  via  $\iota$ . An element of  $(G \times J_{f_0})/J_{f_0}[n](k')$



is represented by a pair  $(g, [D])$  with  $g \in G(k'^s)$ ,  $[D] \in J_{f_0}(k'^s)$  such that for any  $\sigma \in \text{Gal}(k'^s/k')$ ,

$$g^{-1}\sigma g = \sigma[D] - [D] \in J_{f_0}[n](k'^s).$$

Two representatives  $(g_1, [D_1]), (g_2, [D_2])$  are equivalent if and only if there exists some  $[D_0] \in J_{f_0}[n](k'^s)$ , or equivalently in  $J_{f_0}[n](k)$ , such that

$$(g_2, [D_2]) = (g_1, [D_1]) \cdot ([D_0], [D_0]).$$

Denote by  $w_0 \in W_{f_0}(k')$  the image of  $f_0$  via the section  $\kappa_W$ . Then (3.11) is given by

$$\begin{aligned} \gamma : (G \times J_{f_0})/J_{f_0}[n](k') &\rightarrow W_{f_0}(k') \\ (g, [D]) &\mapsto (g, [D]).w_0 = g.(w_0 - [D]). \end{aligned}$$

Clearly  $\gamma$  is Galois equivariant. The major advantage  $\gamma$  has over  $\delta : G \times S \rightarrow V$  is that  $\gamma$  is bijective when  $k'$  is separably closed. Therefore by a descent argument as in the proof of Theorem 1.4,  $\gamma$  is bijective for arbitrary  $k'$ . This straightening suggests comparing measures on  $W$ .

**Lemma 3.6.**  $\theta$  is surjective, each fiber is a principal homogeneous space of  $G(k')$ .

**Proof:** The heuristic is the following long exact sequence

$$1 \rightarrow G(k') \rightarrow W_{f_0}(k') \rightarrow J_{f_0}(k') \rightarrow H^1(k', G),$$

where the last map factors as

$$J_{f_0}(k') \rightarrow J_{f_0}(k')/nJ_{f_0}(k') \rightarrow H^1(k', J_{f_0}[n]) \rightarrow H^1(k', G),$$

which we know is trivial from Axiom II.2.

Rigorously, fix any  $[D] \in J_{f_0}(k')$ , take any  $[D_1] \in J_{f_0}(k'^s)$  such that  $n[D_1] = [D]$ . The 1-cocycle  $(\sigma[D_1] - [D_1])_\sigma \in H^1(k', J_{f_0}[n])$  is the image of  $[D]$  under the Kummer map. By Axiom II.2, its image in  $H^1(k', G)$  is trivial. Therefore, there exists  $g \in G(k'^s)$  such that

$$g^{-1}\sigma g = \sigma[D_1] - [D_1].$$

Then  $\theta((g, [D_1]).w_0) = [D]$ . For any  $g_0 \in G(k')$ ,

$$g_0.(\gamma(g, [D_1])) = (g_0, 0).(g, [D_1]).w_0$$

also does the job.

Conversely,  $(g_1, [D_1]).w_0$  and  $(g_2, [D_2]).w_0$  are two elements of  $W_{f_0}(k')$  mapping to  $[D_0]$ . Put  $[E] = [D_2] - [D_1] \in J_{f_0}[n](k'^s)$ . Then  $g_2[E]^{-1}g_1^{-1} \in G(k')$ , and

$$(g_2[E]^{-1}g_1^{-1}, 0).(g_1, [D_1]).([E], [E]) = (g_2, [D_2]). \quad \square$$

**Remark 3.7.** Suppose  $k'$  is a local field. Fix  $f_0 \in S(k')$ , and  $w_0 = \kappa_W(f_0)$ . Then  $\theta$  sends the  $G(k) \times J_{f_0}(k')$ -orbit of  $w_0$  to  $nJ_{f_0}(k')$ . Suppose  $[D] \in J_{f_0}(k')$  is not divisible by  $n$ . Recall in Axiom II.3, we had a local section  $\kappa_D$  corresponding to the class of  $[D]$  in  $J_{f_0}(k')/nJ_{f_0}(k')$ . Write  $T_D = \kappa_D(f_0)$  and Axiom IV.4 says there exists a  $w_D \in W(k')$  mapping to  $T_D$  via  $\pi$ . Then  $\theta$  sends the  $G(k) \times J_{f_0}(k')$ -orbit of  $w_D$  to  $[D] + nJ_{f_0}(k')$ .

We now restrict to the case when  $k$  is a number field and extend Lemma 3.6 to  $\mathbb{A}_k$  using Axiom III on integral orbits.

**Lemma 3.8.** Suppose  $f_0 = (f_\nu)_\nu \in S(\mathbb{A}_k)$ . Then the map  $\theta : W_{f_0}(\mathbb{A}_k) \rightarrow J_{f_0}(\mathbb{A}_k)$  is surjective.

**Proof:** Given any  $([D_\nu])_\nu \in J_{f_0}(\mathbb{A}_k)$ , there exists some  $(w_\nu)_\nu \in W_{f_0}(\prod_\nu k_\nu)$  mapping to it via  $\theta$ . Write  $T_\nu = \pi(w_\nu)$ . Note  $T_\nu \in V^s(k_\nu)$ . For almost all  $\nu$ ,  $f_\nu \in S(\mathcal{O}_\nu)$  and hence by Axiom III.1 there exists  $g_\nu \in G(k_\nu)$  such that  $g_\nu.T_\nu \in V_{f_0}(\mathcal{O}_\nu)$ . Therefore by definition of  $W(\mathcal{O}_\nu)$ , for almost all  $\nu$ , we can choose  $g_\nu.w_\nu \in W_{f_0, \nu}(\mathcal{O}_\nu)$  mapping to  $[D_\nu]$  via  $\theta$ .  $\square$

**Lemma 3.9.** Suppose  $f_0 = (f_\nu)_\nu \in S'$ , where  $S'$  is defined in Axiom III.2. Then the fiber of the map  $\theta : W_{f_0}(\mathbb{A}_k) \rightarrow J_{f_0}(\mathbb{A}_k)$  is a principal homogeneous space for  $G(\mathbb{A}_k)$ .

**Proof:** Just as in the proof of Lemma 3.6,  $G(\mathbb{A}_k)$  acts on the fibers and clearly if  $(w_\nu)_\nu, (w'_\nu)_\nu \in W_{f_0}(\mathbb{A}_k)$  have the same image, then there exists some  $(g_\nu)_\nu \in G(\prod_\nu k_\nu)$  sending one to the other. We need to show  $g_\nu$  is integral for almost all  $\nu$ . For almost all  $\nu$ ,  $T_\nu = \pi(w_\nu), T'_\nu = \pi(w'_\nu)$  are integral and  $f_\nu \in S'_\nu$ . Therefore by Axiom III.2,  $g_\nu$  is integral.  $\square$

We now fix a measurable subset  $K$  of  $S'$  of finite measure. Denote by  $\mathcal{J}_K(\mathbb{A}_k)$ ,  $V_K(\mathbb{A}_k)$ ,  $W_K(\mathbb{A}_k)$  the corresponding fibers as subsets of the adelic points. The fibers of the maps  $W_K(\mathbb{A}_k) \rightarrow V_K(\mathbb{A}_k), \mathcal{J}_K(\mathbb{A}_k) \rightarrow K$  are the  $\mathbb{A}_k$ -points of abelian varieties, and by giving them the probability measure, one obtains measures  $\nu_1$  on  $W_K(\mathbb{A}_k)$  and  $\mu_0$  on  $\mathcal{J}_K(\mathbb{A}_k)$ .

The above two lemmas imply that  $W_K(\mathbb{A}_k)$  maps surjectively onto  $\mathcal{J}_K(\mathbb{A}_k)$  via  $\theta$  and the fibers are principal homogeneous spaces for  $G(\mathbb{A}_k)$ . This defines another measure  $\nu_2$  on  $W_K(\mathbb{A}_k)$  by taking the tamagawa measure on the fiber.

**Theorem 3.10.**  $\nu_1 = \nu_2$ .

**Proof:** Since every adelic measure in sight is defined as a product measure, it suffices to work over each local completion  $k_\nu$  and  $K$  any measurable subset of  $S(k_\nu)$ . Write  $k'$  for  $k_\nu$ . From Axiom II.3 and II.4, we saw that the measure  $\nu$  on  $V^s(k')$  can be computed fiberwise over  $S(k')$ , hence so can  $\nu_1$ . The measure  $\mu_0$  on  $\mathcal{J}_K(k_\nu)$  is also defined fiberwise over  $K$ , therefore the measure  $\nu_2$  can be computed fiberwise. Fix  $f_0 \in K$ , we are reduced to comparing the two measures  $\nu_1, \nu_2$  on  $W_{f_0}(k')$ .

$$\begin{array}{ccc} J_{f_0}(k') & \longrightarrow & W_{f_0}(k') \\ & & \downarrow \pi \\ & & V_{f_0}(k') \end{array} \quad \begin{array}{ccc} G(k') & \longrightarrow & W_{f_0}(k') \\ & & \downarrow \theta \\ & & J_{f_0}(k') \end{array}$$

More explicitly, for any subset  $E$  of  $W_{f_0}(k')$  and any  $T \in V_{f_0}^s(k'), [D] \in J_{f_0}(k')$ , denote by  $E_T \subset J_{f_0}(k'), E_{[D]} \subset G(k')$  the corresponding fibers of the maps  $\pi : W_{f_0}(k') \rightarrow V_{f_0}^s(k')$  and

$\theta : W_{f_0}(k') \rightarrow J_{f_0}(k')$ . Recall  $\tau_{f_0}$  is the fiber measure on  $V_{f_0}^s(k')$ . Then

$$\begin{aligned}\nu_1(E) &= \int_{\pi(E)} \mu_0(E_T) d\tau_{f_0}(T) \\ \nu_2(E) &= \int_{\theta(E)} \tau(E_{[D]}) d\mu_0([D]).\end{aligned}$$

The unimodular locally compact group  $G(k')$  acts on the locally compact topological space  $W_{f_0}(k')$  with quotient  $J_{f_0}(k')$  and trivial stabilizer. Note this is the titular “straightening” we wished to achieve. The  $G(k')$ -invariant measures on  $W_{f_0}(k')$  are in bijection with their induced measures on  $J_{f_0}(k')$ . Let  $\nu_1^*, \nu_2^*$  denote the induced measures on  $J_{f_0}(k')$ . Then  $\nu_2^* = \mu_0$  by definition.

By Remark 3.7, translation by some  $[D] \in J_{f_0}(k')$  has the effect to moving between soluble orbits. Hence  $\nu_1^*$  is a priori  $nJ_{f_0}(k')$ -invariant from Axiom I, and  $J_{f_0}(k')$ -invariant due to Axiom II.4. Since  $J_{f_0}(k')$  is secretly also a (locally) compact group, there exists some nonnegative real constant  $c_{f_0}$  such that  $\nu_1^* = c_{f_0}\nu_2^*$  and therefore  $\nu_1 = c_{f_0}\nu_2$ . We compute  $c_{f_0}$  by computing the two measures of a model set.

Write  $T_0 = \kappa(f_0)$  and let  $H \subset G(k')$  denote its stabilizer. Then  $H \simeq J_{f_0}[n](k')$ . Let  $K'$  be a compact measurable subset of  $G(k')$  such that  $K'H = K'$ . Let  $K'.T_0 \subset V_{f_0}(k')$  denote the orbit of  $T_0$  under  $K'$ , and let  $E \subset W_{f_0}(k')$  be its pre-image under  $\pi$ . Then

$$\nu_1(E) = \tau_f(E) = \frac{\tau(K')}{|J_{f_0}[n](k')|} \cdot |c|_\nu,$$

where  $c \in k^\times$  is the constant in Lemma 3.1.

The image of  $E$  under  $\theta$  is  $nJ_{f_0}(k')$  and each fiber  $E_{[D]}$  is  $K'$ . Therefore,

$$\nu_2(E) = \frac{\tau(K')}{|J_{f_0}(k')/nJ_{f_0}(k')|}.$$

Combining the two, we get, on the level of fibers,

$$\mu_2 = \mu_1 \cdot \frac{|J_{f_0}[n](k')|}{|J_{f_0}(k')/nJ_{f_0}(k')|} \cdot |c|_\nu.$$

As shown in [17] Lemma 5.7, Lemma 5.14, the quotient  $|J_{f_0}[n](k_\nu)|/|J_{f_0}(k')/nJ_{f_0}(k_\nu)| =: a_\nu$  does not depend on  $f_0$ . Therefore on  $W(k_\nu)$ , we have  $\mu_2 = \mu_1 \cdot a_\nu \cdot |c|_\nu$ .

As one takes the product over all places,  $|c|_\nu$  disappears due to the product formula, so does  $a_\nu$  as in (3.6).  $\square$

We are now in position to prove Theorem 3.3 which we restate for completeness.

**Theorem 3.11.** Suppose  $k$  is a number field. For each finite place  $\nu$ , let  $\mathcal{O}_\nu$  denote the local ring of integers. Let  $K$  be a measurable subset of  $S(\prod_{\nu|\infty} \mathcal{O}_\nu \times \prod_{\nu|\infty} k_\nu)$  be finite measure. Let  $V_K \subset V(\mathbb{A}_k)$  be the soluble preimage. That is  $V_K$  is the intersection in  $V(\prod k_\nu)$  of  $f^{-1}(K)$ ,  $V(\mathbb{A}_k)$  and

$$V^{ls} = \{(T_\nu)_\nu | T_\nu \text{ is in a soluble } k_\nu \text{ orbit, } \forall \nu\}.$$

Suppose Axiom I, II, III, IV are satisfied, then

$$\nu(G(k) \backslash V_K) = \tau(G(k) \backslash G(\mathbb{A}_k)) \cdot \mu(K), \quad (3.12)$$

where the left hand side is computed by taking the measure of a measurable fundamental set.

**Proof:** By removing a measure zero set from  $K$ , we assume  $K \subset S'$ . As before, write  $W_K(\mathbb{A}_k)$  for  $(f \circ \pi)^{-1}(K)$ . Then  $V_K = \pi(W_K(\mathbb{A}_k))$ . If  $F$  is a measurable fundamental set for  $G(k) \backslash V_K$ , then one can take  $\pi^{-1}(F)$  as a measurable fundamental set for  $G(k) \backslash W_K(\mathbb{A}_k)$ . Then

$$\begin{aligned} \nu(G(k) \backslash \pi(W_K(\mathbb{A}_k))) &= \nu_1(G(k) \backslash W_K(\mathbb{A}_k)) && \text{by definition of } \nu_1 \\ &= \nu_2(G(k) \backslash W_K(\mathbb{A}_k)) && \text{by Theorem 3.10} \\ &= \tau(G(k) \backslash G(\mathbb{A}_k)) \mu_0(\mathcal{J}_K(\mathbb{A}_k)) && \text{by definition of } \nu_2 \\ &= \tau(G(k) \backslash G(\mathbb{A}_k)) \cdot \mu(K) && \text{by definition of } \mu_0. \quad \square \end{aligned}$$

### 3.5 Alternative formulation for Axiom IV

In this section, we give an alternative formulation for Axiom IV. There are two main inspiration, namely the difficulty of proving Axiom II.2 encountered in [18], and the fact that in Chapter 1, we not only constructed torsors of Jacobians of hyperelliptic curves, but also a disconnected group with the Jacobian as the identity component and the torsor as another component.

**Lemma 3.12.** Suppose Axioms I, II.1, IV.1-3 hold. For any field  $k'$  over  $k$  and  $T \in V_{f_0}(k')$ , let  $W_T$  denote the fiber of  $W \rightarrow V$ . Then there exists a morphism

$$\varphi_T : W_T^n := W_T \times W_T \times \cdots \times W_T \rightarrow J_{f_0}$$

of  $J_{f_0}$ -torsors. This morphism is compatible with the action of  $G$  in the following sense: if  $g.T = T' \in V(k')$ , denote by  $g : W_T \rightarrow W_{T'}$  induced from the action of  $g$  on  $W$ , let  $g^n$  denote the map from  $W_T^n$  to  $W_{T'}^n$ , then  $\varphi_{T'} \circ g^n = \varphi_T$ . Moreover,

$$\kappa_W(f_0) = w_0 \in W_{T_0}[n] := \{w \in W_{T_0} \mid \varphi_{T_0}(w, \dots, w) = 0\}. \quad (3.13)$$

**Proof:** Recall we had a Galois-equivariant isomorphism,

$$\gamma : \frac{G \times J_{f_0}}{J_{f_0}[n]}(k') \rightarrow W_{f_0}(k').$$

Fix some  $g_0 \in G(k'^s)$  such that  $g_0.T_0 = T$ . For any  $w \in W_T(k'^s)$ , one can choose a unique representative of  $\gamma^{-1}(w)$  in  $G(k'^s) \times J_{f_0}(k'^s)$  of the form  $(g_0, [D_w])$ . Then we define, for  $w_1, \dots, w_n \in W_T(k'^s)$ ,

$$\varphi_T(w_1, \dots, w_n) = [D_{w_1}] + \cdots + [D_{w_n}].$$

Choosing a different  $g_0$  amounts to changing each  $[D_w]$  by a fixed element in  $J_{f_0}[n](k'^s)$  which does not change  $\varphi$ . Compatibility with the actions of  $J_{f_0}$  and  $G$  follows directly from the definition of the action of  $G \times \mathcal{J}$  on  $W$ . (3.13) follows since  $[D_{w_0}] = 0$ .  $\square$

**Lemma 3.13.** Suppose Axioms I, II.1, IV.1-3 hold. For any field  $k'$  over  $k$  and for any  $T \in V_{f_0}(k')$ , let  $\psi_T : W_T(k') \rightarrow J_{f_0}(k')$  denote the map on  $k'$ -points of  $\varphi \circ \Delta$  where  $\Delta$  is the diagonal embedding of  $W_T$  into  $W_T^n$ . Then  $W_T(k')$  is non-empty if and only if the class in  $H^1(k', J_{f_0}[n])$  corresponding to the  $k'$ -orbit of  $T$  lies in the image of the Kummer map. In fact, it is the image of  $\psi_T(w)$  for any  $w \in W_T(k')$ .

**Proof:** Suppose  $w \in W_T(k')$ , write  $(g, [D]) = \gamma^{-1}(w)$ . Then  $\psi_T(w) = n[D] \in J_{f_0}(k')$  and for any  $\sigma \in \text{Gal}(k'^s/k')$ ,

$$g^{-1}\sigma g = (\sigma[D] - [D])_\sigma = \text{image of } n[D] \text{ under the Kummer map.}$$

Conversely, if the image of the Kummer map of  $[D'] \in J_{f_0}(k')$  corresponds to the  $k'$ -orbit of some  $T \in V(k')$ , take any  $[D] \in J_{f_0}(k'^s)$  such that  $n[D] = [D']$ . The cocycle  $(\sigma[D] - [D])_\sigma$  becomes trivial in  $H^1(k', G)$ . Thus, there exists  $g \in G(k'^s)$  such that  $\sigma[D] - [D] = g^{-1}\sigma g$ . Then  $\gamma(g, [D]) \in W_T(k')$ .  $\square$

**Corollary 3.14.** Assuming Axioms I, II.1, IV.1-3, then Axiom II.2 implies Axiom IV.4.

**Axiom IV': (Torsor of  $\mathcal{J}$  with a fixed lift)** Let  $W \xrightarrow{\pi} V$  be a torsor for  $\mathcal{J} \times_S V$  as a  $V$ -scheme, such that

1.  $G$  acts on  $W$  equivariantly with respect to  $\pi$ ,
2. for any field  $k'$  over  $k$  and  $T \in V_{f_0}(k')$ , there exists a  $G$ -equivariant morphism

$$\varphi_T : W_T^n := W_T \times W_T \times \cdots \times W_T \rightarrow J_{f_0}$$

of  $J_{f_0}$ -torsors and a section  $\kappa_W : S \rightarrow W$  such that  $\kappa_W(f_0)$  lands inside  $W_{T_0}[n]$  as defined in (3.13),

3. the actions of  $G \times V$  and  $\mathcal{J} \times_S V$  on  $W$  commute and coincide on the common  $\mathcal{J}[n] \times_S V$ ,

4. for any field  $k'$  over  $k$ , the images of the maps

$$W_T(k') \xrightarrow{\psi_T} J_{f_0}(k') \rightarrow J_{f_0}(k')/nJ_{f_0}(k') \quad (3.14)$$

as  $T$  runs in  $V_{f_0}(k')$  cover the entire  $J_{f_0}(k')/nJ_{f_0}(k')$ .  $\square$

**Proposition 3.15.** Axioms I, II, IV.1-3 together is equivalent to Axioms I, II.1, IV'.

**Proof:** We have proven the forward direction. Suppose now Axioms I, II.1, IV' hold. It remains to check Axioms II.2 and IV.4. Corollary 3.14 implies that only checking II.2 is enough, but our argument proves both at the same time.

Fix any  $T \in V_{f_0}(k')$ , define  $W_T[n]$  similarly as in (3.13) as the kernel of  $\varphi \circ \Delta$ . Then  $W_T[n]$  is a  $J_{f_0}[n]$ -torsor and hence corresponds to a class  $c_T \in H^1(k', J_{f_0}[n])$ . We claim that  $c_T$  also corresponds to the  $k'$ -orbit of  $T$ .

Indeed, choose  $g \in G(k'^s)$  such that  $g.T_0 = T$ . Write as usual  $w_0 = \kappa_W(f_0) \in W_{T_0}[n](k')$ , then  $G$ -equivariance implies that  $g.w_0 \in W_T[n](k'^s)$ . For any  $\sigma \in \text{Gal}(k'^s/k')$ ,

$$\sigma(g.w_0) = (\sigma g g^{-1})(g.w_0).$$

Thus,  $\sigma g g^{-1}$  is the element in  $\text{Stab}_G(T)(k'^s)$  sending  $g.w_0$  to its  $\sigma$ -conjugate. Let  $\iota_T : J_{f_0}[n] \hookrightarrow G$  denote the identification of  $J_{f_0}[n]$  with  $\text{Stab}_G(T)$ . Then  $c_T = (D_\sigma)_\sigma$  where  $\iota_T(D_\sigma) = \sigma g g^{-1}$ . To see what  $k'$ -orbit  $c_T$  corresponds to, we need to look at the image of  $c_T$  in  $H^1(k', G)$ . Recall the map  $H^1(k', J_{f_0}[n]) \rightarrow H^1(k', G)$  is induced by  $\iota_{T_0} : J_{f_0}[n] \hookrightarrow G$  and by Axiom I.1,

$$\iota_{T_0}(D_\sigma) = g^{-1} \iota_T(D_\sigma) g = g^{-1} \sigma g,$$

confirming our claim.

By definition, the image of  $c_T$  in  $H^1(k', J_{f_0}[n])$  is the class corresponding to the  $J_{f_0}$ -torsor  $W_T$ . Therefore,  $W_T(k') \neq \emptyset$  if and only if  $c_T$  lies in the image of the Kummer map. Suppose  $w \in W_T(k')$ , there exists a unique  $[D] \in J_{f_0}(k'^s)$  such that  $w = g.w_0 + [D]$ . Since  $\varphi$  is a map of



$J_{f_0}$ -torsors,  $\psi_T(w) = n[D] \in J_{f_0}(k')$ . Moreover,  $c_T = ([D] - [D]^\sigma)_\sigma$  since  $w$  is rational. Therefore,  $c_T$  is the Kummer image of  $-n[D]$ . Hence there is a bijection between the images of maps defined in (3.14) and the subset of elements in  $J_{f_0}(k')/nJ_{f_0}(k')$  whose images in  $H^1(k', J_{f_0}[n])$  correspond to orbits. Therefore Axiom IV'.4 implies II.2 and IV.4.  $\square$

# References

- [1] M. Bhargava and B. Gross. Arithmetic invariant theory. 2012. arXiv:1206.4774.
- [2] M. Bhargava and B. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational weierstrass point. 2012. arXiv/1208.1007.
- [3] M. Bhargava and W. Ho. Average sizes of Selmer groups in families of elliptic curves. In preparation.
- [4] M. Bhargava and W. Ho. Coregular spaces and genus one curves. In preparation.
- [5] M. Bhargava and A. Shankar. Binary quadric forms having bounded invariants, and the boundedness of the average rank of elliptic curves. 2010. arXiv/1006.1002.
- [6] U. V. Desale and S. Ramanan. Classification of vector bundles of rank 2 on hyperelliptic curves. *Inventiones Mathematicae*, 38(2):161–185, 1976/77.
- [7] R. Donagi. Group law on the intersection of two quadrics. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, 7(2):217–239, 1980.
- [8] L. Gauthier. Footnote to a footnote of André Weil. *Rend. Sem. Mat. Torino*, 14:325–328, 1954–55.
- [9] J. Harris. *Algebraic geometry - a first course*. 1992.
- [10] R. Hartshorne. *Algebraic geometry*. 1977.
- [11] W. Ho. Orbit parametrizations of curves. 2009. Ph.D thesis (Princeton).

- [12] D. Mumford. *Abelian Varieties*. 1970.
- [13] B. Poonen. Average rank of elliptic curves. *Séminaire Bourbaki*. Exposé 1049.
- [14] B. Poonen and E. Rains. Self cup products and the theta characteristic torsor. 2011. arXiv:1104.2105.
- [15] B. Poonen and E. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.
- [16] M. Reid. The complete intersection of two or more quadrics. 1972. Ph.D thesis (Trinity College, Cambridge).
- [17] E. Schaefer. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica*, XCVIII.3, 2001.
- [18] J. Thorne. Some canonical constructions in arithmetic invariant theory. Submitted.
- [19] E. Vinberg. The weyl group of a graded lie algebra. *Math. USSR-Izv.*, 10:463–495, 1976.
- [20] A. Weil. *Oeuvres Scientifiques/Collected Papers*. 1980.